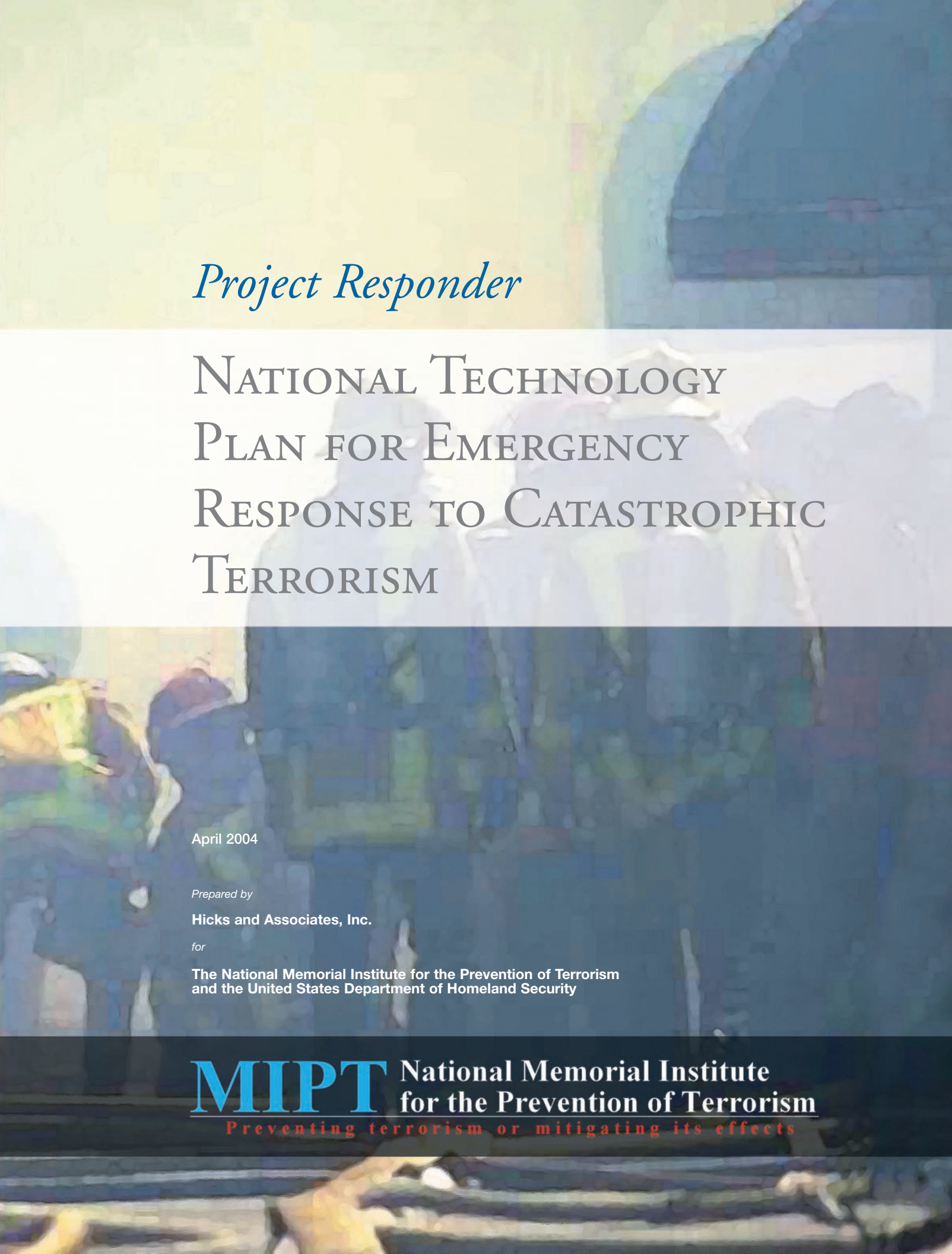


Project Responder

National Technology Plan for Emergency Response to Catastrophic Terrorism

April 2004

Prepared by

Hicks and Associates, Inc.

for

The National Memorial Institute for the Prevention of Terrorism and the United States Department of Homeland Security

MIPT National Memorial Institute for the Prevention of Terrorism

Preventing terrorism or mitigating its effects

Project Responder

National Technology Plan for Emergency Response to Catastrophic Terrorism

Edited by

Thomas M. Garwin, Neal A. Pollard, and Robert V. Tuohy

April 2004

Prepared by

Hicks and Associates, Inc.

for

**The National Memorial Institute for the Prevention of Terrorism
and the United States Department of Homeland Security**

Supported under Award Number MIPT106-113-2000-002, Project Responder
from the Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT)
and the Office of Domestic Preparedness, Department of Homeland Security.

Executive Summary

Purpose and Vision – Project Responder

The National Memorial Institute for the Prevention of Terrorism (MIPT) in Oklahoma City focuses on "preventing and deterring terrorism or mitigating its effects." Since April 2001, MIPT has supported Hicks & Associates, Inc. in developing a National Technology Plan for Emergency Response to Catastrophic Terrorism, pursuant to a guiding vision:

> *Emergency responders should have the capability to prevent or mitigate terrorist use of chemical, biological, radiological, nuclear, or high explosive/incendiary (CBRNE) devices and emerging threats.*

In addition to the specifics of CBRNE devices and emerging threats, responders need to be prepared to deal with the catastrophic scale of effects that these threats may produce; thus a need for technologies to rapidly coordinate and integrate response capabilities from multiple local, regional, state, and federal organizations and disciplines is implicit in this vision.

The plan focuses on technology investment to improve capabilities within twelve National Terrorism Response Objectives (NTROs) that cover the anticipated scope of emergency responders' requirements for dealing with chemical, biological, nuclear, radiological, and explosive/incendiary attacks on the homeland:[1]

- Personal Protection and Equipment
- Detection, Identification, and Assessment
- Unified Incident Command, Decision Support and Interoperable Communications
- Response and Recovery
- Emergency Management Preparation and Planning
- Medical Response
- Public Health Readiness for Biological Agent Events
- Logistics Support
- Crisis Evaluation and Management
- All-Source Situational Understanding
- Criminal Investigation and Attribution
- Mitigation and Restoration for Plant and Animal Resources

Strategy for Responder Capability Improvement

Developing a technology plan to fill gaps in responder capability is important but it will not be enough by itself to actually increase emergency responder capability across the nation. In many areas, responder capabilities are limited more by resources and gaps in organizational capability than by technology.

Organizations responsible for improving responder readiness for catastrophic events need to develop a strategy for implementing the technology plan and assuring the successful transition of new technology into the hands of emergency responders. Those organizations should consider the lessons learned by other agencies who have

[1] The National Terrorism Response Objectives resulted from a series of eight workshops and dozens of field interviews with over 125 emergency responders, a number of related groups established to focus on terrorism response, and 135 experts in key technology fields from across government, industry, and academia.

managed similar activities, together with the unique characteristics of responder organizations.

The following ten imperatives capture the main elements of an implementation strategy that empowers responders and meshes *the need for a research and development program led by the federal government with the decentralized nature of responder procurement decision-making:*

- Establish and exploit appropriate responder collaborative environments.
- Focus federal, industrial, and non-profit investment on the most pressing needs articulated by responders.
- Insist on affordable end-products.
- Leverage existing federal, state, and local government investment and infrastructure.
- Where possible, include terrorism response capability into upgrades of normal duty clothing and equipment.
- Achieve continual improvement through spiral development and evolutionary deployment.
- Emphasize open architecture, interoperability, and proactive involvement in establishing appropriate standards and testing.
- Identify existing commercial and government advanced technologies for integration into innovative solutions to meet responder needs.
- Quicken the maturation and deployment of advanced technology products, innovative concepts and eventual capabilities through modeling and simulation, demonstrations and effective commercialization.
- Focus investment in strategic research areas to provide future opportunities.

Furthermore, although the vision and resultant plan are for response to catastrophic terrorism, technology development to increase responder capability should aim, when possible, for increases in "all-hazards" capability. That is, technology development should improve responders' capabilities to deal with all types of catastrophes, whether man-made, natural, or accidental.

Response Technology Objectives – A National Agenda for Research and Development

Each NTRO chapter in this plan presents technology roadmaps made up of new initiatives to close gaps in responder capabilities. The building blocks for the roadmaps are Response Technology Objectives (RTOs). The RTOs recommend programs for the federal government to adopt (in addition to current efforts), and most are linked to the prioritized needs of emergency responders. The 48 RTOs described herein include descriptions of the objective and its goals, the payoffs that will result from the RTO, challenges that will be encountered while pursuing the RTO, and milestones and metrics by which developers can structure a program and gauge its progress. Taken as a whole, the 48 RTOs may be considered a research and development agenda for improving emergency response capabilities.

Each RTO also includes rough budget estimates and a programmatic timeline. The different budgets represented in the 48 RTOs sum to a total of nearly $3.5 billion, over six years. However, these totals are neither definitive nor comprehensive. The cost and schedule estimates assume the continuation of currently programmed efforts in related areas and assume effective leveraging of those programs. Furthermore, the estimates are based on top-down expert judgment rather than a detailed bottom-up plan. More precise estimates would require knowledge of the actual budgetary and institutional environment in which the work is to be carried forward. Finally, these estimates concentrate on needed technology research and development: they do not include costs for establishing standards, third party testing and evaluation, acquisition, training, maintenance, and the myriad other actual costs that will be encountered in increasing the capabilities of state and local responders. What these estimates do provide is a minimum threshold investment in

research and development that the nation must pursue, if it is to have the option of increasing response capabilities consistent with the goals, needs, priorities, and technology objectives described herein.

The RTOs, grouped by National Terrorism Response Objective, are:

Personal Protection and Equipment (PPE)

- *Body Protection* – Devise new concepts for improved body protection and create the basis for prototypes. The ultimate goal is to provide the basis for a one-suit-meets-all-goals system.
- *Respiratory Protection - Oxygen Available* – Discover and demonstrate new materials and filter and mask designs to achieve longer duration, lighter weight, with effectiveness against all toxins, low breathing resistance, and a cost of less than $300 per unit.
- *Respiratory Protection - Oxygen Deficient* – Discover new air storage concepts and improved materials for self-contained breathing apparatus. Increase in-service time from less than one hour to four hours.
- *Decontamination* – Discover and demonstrate new ways to neutralize toxins on responders clothing and gear. Explore more environmentally friendly chemical wash systems that are quick and thorough. Find means of determining the completeness of decontamination.
- *Escape Respiratory Protection* – Develop an improved version of escape hood: more compact, lighter, with a shelf-life of five years, and effective against all hazards.

Detection, Identification, and Assessment (DIDA)

- *Wearable Integrated CBR Sensors* – Develop miniature, integrated CBR detectors and collection devices for use on responders, and eventually the general population. Provide rapid (timely) alert to the wearer of danger and type of attack, *e.g.*, proceed to decontamination, administer prophylaxis, take antibiotic, "suit up" or don mask.
- *Stand-off Radiation Detection and Identification* – Develop affordable, robust radiation detectors for stand-off discrimination and identification of nuclear weapons and dirty bombs. Sensors must be capable of networked operation and detecting unshielded nuclear weapons in vehicles moving at highway speeds.
- *Integrated Remote Detection of CB Agents* – Develop and demonstrate compact, low-cost, reliable sensor technologies and/or systems for wide area, remote detection of airborne clouds and plumes of biological and chemical agents. Such systems should be able to reliably detect and accurately characterize threat aerosol clouds at ranges of up to 1 kilometer.
- *Portable Stand-off Container Inspection* – Develop and demonstrate compact, non-contact, non-intrusive sensor technologies and/or systems for detection of biological and chemical agents in sealed containers. Such systems should be able to reliably detect and potentially characterize threat agents in containers at distances of 1-2 meters.
- *Integrated Networked Sensors for CBRNE Detection* – Develop two or more large-scale urban networked sensor testbeds to support the full spectrum of DIDA functions. Employ arrays of static, mobile, and remote sensors for intercepting nuclear and radiological weapons, detecting and characterizing aerosolized CB agents, and mapping the attack and ensuing effects. Integrate sensor networks with information networks for flow of raw data, indications, and warning.
- *Combined Effects Modeling for Urban Canyons* – Integrate CBRNE effects models and simulations for complex urban canyons. The models should provide inputs and outputs to help in medical and population monitoring data, as well as provide inputs to models associated with injury and casualty assessment.

- *Research for On-Scene Assessment of Low-Dose Exposure to Chemical Agents* – Research and develop the feasibility of sensor systems that can reliably determine at the scene of an attack whether an individual has symptoms caused by low-dose exposure to a chemical warfare agent.

- *Real-Time Structural Stress Measurement* – Develop a portable, real-time stress measurement sensor for continuous onsite assessment of structural safety. After a blast associated with terrorist event, responders may need to enter structures or rubble without knowing whether collapse is imminent. During rescue and response, the safety of the structure or rubble may change.

- *Stand-off Automatic Choke Point Screener* – Develop sensor systems that can find and intercept terrorists at choke points (building entrances, airports, etc.) prior to their intended attack, or after an attack as they attempt to escape.

Unified Incident Command Decision Support and Interoperable Communications (UIC)

- *Point Location and Identification* – Develop a system for the location of responder personnel in three dimensions in the incident area (*i.e.,* in buildings and rubble piles).

- *Seamless Connectivity and Information Assurance* – Develop a "Responder C^3 System" that can seamlessly and dynamically interconnect multiple interagency users, who have multiple functions, multiple information and communications systems. The systems must operate the first time and every time and remain operational through the incident.

- *Incident Command Information Management and Dissemination* – Provide incident command decision support, situation and resource status management, communications system management and mission/task tracking. This capability should include information visualization and fusion tools as well as modeling and simulation capability.

- *Multimedia Supported Telepresence* – Adapt current Web-based technologies to the responder environment in order to obtain multimedia information (*i.e.,* enhanced teleconferencing) on a timely basis.

Response and Recovery (R&R)

- *Contaminated Victim Knowledge Base* – Develop a tool for emergency responders to use in determining how to respond to a mass chemical, biological or radiation contamination event. Using data provided by available sensors and information stored before the event the, tool will provide responders with the best course of action to begin the decontamination of large numbers of victims.

- *Protective Coatings for Critical Equipment* – Develop materials and appliqués that will resist contamination or facilitate rapid decontamination without degrading sensitive equipment such as electronics, such that critical equipment can be rapidly returned to service within the contaminated zones in less than one hour.

- *Ground Penetrating Radar for Specialized Search and Rescue* – Develop and demonstrate an affordable ground penetrating radar system to assist search and rescue operations, in order to rapidly locate, assess, and rescue, injured and/or contaminated victims.

- *Irradiation and Gaseous Decontamination for Mass Fatalities* – Adapt irradiation and gaseous decontamination technologies and methods (*e.g.*, food irradiation and concepts used on postal facilities after October 2001 anthrax attacks, etc.), for mobile use in a mass fatality incident.

Emergency Management Preparation and Planning (EMPP)

- *Risk Awareness and Assessment Decision Support Technology Demonstration* – Integrate existing technology to develop a system that will provide automated decision aides for those charged with assessing the vulnerability and

protective course of action for potential targets within their jurisdictions.

- *Electronic Transcript Smart Card* – Demonstrate, for standardization and acceptance, a digital smart card/chip "electronic transcript" system that securely verifies ID, levels of training/certification, and currency, for the multitude of responders that converge on the scene of a catastrophic event.

- *Alternate/Mobile Hospital Contingency Management* – Develop standards based on case studies, benchmarking, and best practices in use for managing hospital/medical contingencies.

- *Course-of-Action Development System* – A Computer-based decision support and information management tool that can assist the emergency planner/response community in achieving higher levels of sophistication in information assessment, integration and manipulation.

Medical Response (MR)

- *Mass Prophylaxis Knowledge Base and Decision Aid* – Develop a tool for emergency responders to use in determining the "at-risk" population in a mass chemical, biological or radiation contamination event and developing a mass prophylaxis course of action.

- *Mass Prophylaxis Delivery System* – Develop a tool that allows responders to significantly increase the throughput of individuals who are receiving prophylactic treatment.

- *Casualty Management System* – Develop a tool for emergency responders to use to manage potentially tens of thousands of victims from a mass casualty event. The systems should be able to positively track each patient either through tagging (*i.e.,* bar code) or through biometrics. The system should provide the medical/syndromic and treatment records as well as the physical location of the patient.

- *Telemedicine Test Bed* – Establish a telemedicine testbed where research on new concepts of operation and new enabling technology can be explored to support disasters and mass casualty incidents. Conduct research on how quickly doctors can screen patients via telemedicine.

- *Novel Decontamination* – Conduct research to develop new ways to effectively decontaminate large number of victims in the event of a chemical or biological attack, especially in cold weather. It should significantly increase the throughput of people being contaminated and will probably save lives.

Public Health Readiness for Biological Agent Events (PHRBAE)

- *Health Surveillance for Early Detection of Biological Agent Events* – Develop a comprehensive surveillance system that ensures initial recognition of an emergent illness at the earliest point in the progress of a biological agent event. This system would be based in metropolitan areas and the states but would allow fully transparent data aggregation up to the national level.

- *Rapid High-Throughput Clinical Assessment and Testing* – Develop a system that can screen patients through minimally invasive techniques to improve the speed, throughput, comprehensiveness, and convenience of field clinical assessment and testing for biological agent exposure and disease status.

- *Models for Re-dissemination and Contagion of Bio-agents* – Develop improved models for the re-dissemination and contagion of biological agents. The models must be integrated with surveillance information to help get a starting point for the model.

Logistics Support (LS)

- *Integrated Logistics Information System (ILIS)* – Develop an evolutionary Integrated Logistics Information System capable of connecting all echelons of command (including regional and national) and all types of suppliers and other logistics nodes. The functions of this information system include planning and

providing the appropriate initial logistics response to support emergency response to disasters, tracking inventories and items in transit (across jurisdictions), projecting needs for consumables and other support items including transportation, providing information and decision support for transportation optimization, and providing information relevant to the rapid assessment of safe bases of operation.

- *Many-to-Many DNA Matching of Body Parts* – Develop the capability to recover, track, and identify using DNA comparisons of bodily remains from mass casualty events.

Crisis Evaluation and Management (CE)

- *Non-Lethal Safe Seizure of Perpetrators* – Develop non-lethal technologies to instantly immobilize perpetrators with weapons or hostages, such that explosive devices or other weapons are not setoff.

All-Source Situational Understanding (ASU)

- *All-Source Information Fusion and Analysis System* – Develop a prototype tool and doctrinal template for an information and analysis cell to support Incident Command. The objective is to collect, fuse, analyze and present information from all sources, including sensitive intelligence information.

Mitigation and Restoration for Plant and Animal Resources (MRPA)

- *Plant and Animal Responder's Decision Aid* – Allow plant and animal responders to apply codified knowledge and to reach back to specialists so that they will act to most efficiently assess and identify damage, limit onward contamination, and embark on the correct mitigation strategy where plants and animals are the targets or initial indicators of terrorism.

- *Field Screening and Assessment Tests* – Develop a cost-effective set of rapid screening and identification tests for plant and animal disease and the presence of CBR agents in plant and animals.

- *Overhead Imaging for Wide-Area Surveillance and Assessment* – Exploit existing imaging technology involving earth orbit satellite and unmanned surveillance aircraft to remotely survey agricultural terrain for the presence of crop plant disease, down livestock, and wildlife remains.

- *Trace-Back Capabilities Using Information Systems and Tags* – Design and implement a systems approach to using miniaturized chip technology for tracking plant, animals and food products back to points-of-origin with data updating at critical control points.

- *Threat Analysis Critical Control Points Program for the Food Chain* – Use systems analysis to identify the key points in the food chain at which detection is to be attempted and the detection techniques and technologies (including visual inspection) that would be most cost effective.

- *Modeling of Plant and Animal Outbreaks, Surveillance, and Response* – Develop modeling tools for use by cognizant agencies and incident commanders that can aid in optimizing plant and animal surveillance and response strategies.

- *Improved Irradiation Methods* – Find quick, effective and inexpensive prophylactic and post-exposure treatment countermeasures for contaminations and infestations in food and feed through different forms of irradiation.

- *Enhanced Fumigation Technology* – Codify the state of the art in using fumigation to decontaminate food processing and storage facilities and transportation carriers and find cheaper and more efficient ways to perform this function.

- *Digesters and Plasma Burners* – Evaluate the state of the art of portable systems for carcass disposal and develop a program for ascertaining the relative strengths and weaknesses of the individual systems and their operational

capacities, limitations, and costs of procurement and operation in representative field settings. The purpose is to understand our domestic capability to destroy animal carcasses contaminated with threatening diseases.

- *Prototype Prefabricated Animal Crematorium Facility* – A prefabricated system that could be erected and made operational in a matter of several days should be developed to prevent contagion from animal carcasses.

The Long View – Strategic Research for Emergency Response

Within many of the NTROs, responders identified desired capabilities that technologists assessed to be not achievable within the current state of basic science and technology. The project identified five strategic research areas that hold the potential to provide the understanding and techniques that may permit breakthroughs in capabilities. At the basic level envisioned for these research areas, specific research projects are at most loosely connected to specific responder needs; rather the goal is to increase the pool of knowledge that may be drawn upon by development activities in the future.

The five Strategic Research Areas are:

Nanotechnology – Building structures at the molecular level to meet desired goals in the performance of materials for personal protection and equipment. Potential improvements in Personal Protection and Equipment motivated the definition of this SRA. However, its benefits will also contribute to capability increases in Detection, Identification, and Assessment; Unified Incident Command Decision Support and Interoperable Communications; and Response and Recovery.

Surface Science – Central to capability increases in personal protective materials is strategic research and development in the chemistry and physics of surfaces, especially modified surfaces. Surface Science is also relevant to decontamination and to many advanced detector technologies.

Observables and Sensing for Stand-off Inspection of Containers with Chemical or Biological Agents – Discovery and development of revolutionary approaches to rapid, non-intrusive stand-off detection and identification of chemical and biological agents in packages and containers, with effective ranges of a few feet in unconstrained geometry. Strategic research and development in this area will also benefit numerous functional capabilities, described in other NTROs, that require indication or assessment of the presence of chemical or biological agents.

Ultra Wideband (UWB) Communications – Achieving communications penetration through walls, in high rise buildings and underground or in tunnels. Research in this field will support functional capabilities in Unified Incident Command Decision Support and Interoperable Communications, as well as functional capabilities in other NTROs that require communications or telemetry, especially through mass such as collapsed rubble or in areas where commercial wireless communications cannot function today.

Biomarkers of Agent Induced Disease and Systemic Injury in Humans, Plant and Animals – This research area is central to Public Health Readiness for Biological Agent Events and Medical Response, and also to Mitigation and Restoration for Plant and Animal Resources. However, its benefits are also generally important to the Detection, Identification, and Assessment NTRO, and specifically to functional elements in several NTROs that require the identification and assessment of biological and chemical agents. The central thrust is better understanding of changes in living systems under assault by chemical and biological attack, to permit more rapid assessment, agent identification, and treatment selection.

This National Technology Plan is intended to be a draft of a living document. Federal technology planners should not simply fund and implement the plan as written because:

- it needs to be interrelated to other capability areas for efficient application of resources;
- it needs to be iterated as new information becomes available; and

- the appropriate mechanisms for involving commercial vendors in developing technologies and deploying the resulting products to disparate responders have not been worked out.

Thus these technology plans, and the needs that underlie them, will not be the final word on responders' needs and capabilities. Capabilities and needs continually change, and the plan must evolve in response to new R&D results as well as to operational innovations. The goals and objectives of this and subsequent documents should be considered just that—goals—not threshold or exit criteria for capability development. As capabilities are built and fielded, this plan will change. As new threats emerge, needs will change, requiring further changes to the plan. Thus, this plan should be considered the first contribution in an iterative process to the continual improvement of responders' capabilities via an evolutionary development and deployment process that will work in the dispersed responder marketplace.

Preface

The National Memorial Institute for the Prevention of Terrorism (MIPT) in Oklahoma City focuses on "preventing and deterring terrorism or mitigating its effects." Since April 2001, MIPT has funded Project Responder, an effort by Hicks & Associates, Inc. and the Terrorism Research Center, Inc., aimed ultimately at improving local, state and federal emergency responders' capabilities for mitigating the effects of chemical, biological, radiological, nuclear or explosive/incendiary (CBRNE) terrorism. Project Responder will achieve this aim by producing two tools: a National Technology Plan for Emergency Response to Catastrophic Terrorism, and a Web-based Responder Knowledge Base of current and emerging systems and technologies for response to terrorism.

This document builds upon the foundation laid by the first Project Responder Interim Report *Emergency Responders' Needs, Goals, and Priorities* (March 2003)[2], which presented priorities for technology-enabled improvements in response capability, described in twelve National Terrorism Response Objectives (NTROs):

- Personal Protection and Equipment (PPE)
- Detection, Identification, and Assessment (DIDA)
- Unified Incident Command, Decision Support and Interoperable Communications (UIC)
- Response and Recovery (R&R)
- Emergency Management Preparation and Planning (EMPP)
- Medical Response (MR)
- Public Health Readiness for Biological Agent Events (PHRBAE)
- Logistics Support (LS)
- Crisis Evaluation and Management (CE)
- All-Source Situational Understanding (ASU)
- Criminal Investigation and Attribution (CI)
- Mitigation and Restoration for Plant and Animal Resources (MRPA)

The National Terrorism Response Objectives are the result of a series of eight workshops and dozens of field interviews with over 125 emergency responders and a number of related groups established to focus on terrorism response. The objectives cover the anticipated scope of emergency responders' requirements for dealing with chemical, biological, nuclear, radiological, and explosive/incendiary attacks on the homeland. The technology plans for each of the NTROs were developed from a common philosophy that meshes the decentralized nature of responder procurement decision-making with the need for a research and development program led by the federal government.

This draft National Technology Plan is intended to be a living document. Federal technology planners could not simply fund and implement the plan as written because:

- it needs to be interrelated to other capability areas for efficient application of resources;

[2] Neal A. Pollard, Robert V. Tuohy, and Thomas M. Garwin, *Emergency Responders' Needs, Goals, and Priorities*, (March 2003, Updated) an Interim Report of Project Responder, prepared by Hicks and Associates, Inc., for The Oklahoma City National Memorial Institute for the Prevention of Terrorism and the National Institute of Justice of the U.S. Department of Justice, at the request of the U.S. Department of Homeland Security.

- it needs to be iterated as new information becomes available; and
- the appropriate mechanisms for involving commercial vendors in developing technologies and deploying the resulting products to disparate responders have not been worked out.

These three reasons are elaborated in the following paragraphs.

Need for Interrelationship with Other Program Areas – The plan's focus on the needs of emergency responders, while crucial, is not complete. It was very important to discipline the process by addressing the needs of this crucial user community that is on the front line of our national effort against terrorism, and that traditionally has not been intensively supported by new technology development. However, even with a flexible definition of "emergency responder" (for example, to include public health specialists and various types of medical personnel, in some cases of biological attack), important areas of technology development for deterring and preventing terrorism and mitigating its effects are not within the current scope of this plan. Thus, much of port, border, and aviation security, as well as the development of vaccines and medical treatments, is not addressed in the current planning effort.

Moreover, there are important overlaps and synergies between some technologies identified as important for emergency response and those in these other areas. Thus the Project Responder draft National Technology Plan needs to be synchronized with technology planning efforts in these other areas, as well as with other agencies, for maximum efficiency and effectiveness in an overall investment strategy. The Department of Defense already has a number of technologies that address responders' needs. For example, the Combatting Terrorism and Force Protection technologies and demonstrations of Defense Department's Joint Warfighting Science and Technology Plan are relevant to some of the critical needs of emergency responders, and the Technical Support Working Group has produced prototype technologies that would be useful to emergency responders.

Need for Iteration – The experience of federal government and industry best-practice technology planning efforts strongly suggests that technology planning needs to be an iterated, participative process. Detailed budgets can only realistically be developed through a dialog with a selected executing agency, and the amount of money to be allocated to a particular project in a particular period can only be decided in the context of the overall resources that are made available. The planning process itself develops additional information and understanding over time as research and technology programs proceed.

Technology Transfer and Commercialization – Concepts for technology transfer and commercialization are central to any federal strategy for developing and deploying new capabilities to state and local responders. Many issues inherent in successful diffusion of new technology to responders are not technological, but rather range from issues of training, logistics and budgets to basic issues of federalism. Nevertheless, technology transfer, primarily through commercialization, will be important to bring mature technologies into responder-oriented applications or demonstrations, to guarantee to vendors a marketplace sufficient to induce full production of technologies, and to field technologies on a wide enough scale to meet responders' needs. Commercialization strategies – whether through regional purchasing arrangements, public/private partnerships, direct federal acquisition, tied grant programs or other approaches – will be crucial for bringing down costs of new capabilities sufficiently for medium- and smaller-size jurisdictions to procure them.

Another important set of judgments that will affect how technology will be deployed, and thus how it should be developed, relates to the distribution of capabilities at different levels of response. Federal officials and their state and local counterparts will have to determine the most effective distribution and organization of capabilities across the country and at various

levels (*i.e.*, local, state, federal or regional). For example, some specialized capabilities would be most effective and efficient deployed and operated as a regional resource, while other capabilities must be available at the local city or county level. Even within local forces, some capabilities will be given to every responder, while others will be reserved to special units.

Judgments of what capabilities belong at which levels cannot be made *a priori*. Rather they are the result of a set of balancing considerations that are in many ways dependent on technology. Typically, specialized capabilities are unique to specialized organizations because of high cost and difficult training requirements. In some instances technology can reduce cost and training requirements or improve safety to the point that a hitherto specialized capability can be widely distributed. Experiments (technical and operational, aimed at learning) and demonstrations (aimed at determining feasibility) involving innovative concepts, products, advanced technology, systems, and "systems of systems" will be useful in arriving at appropriate, affordable operational applications of new technology, and will stimulate both vendor supply and responder demand for these solutions.

A process to improve responder capabilities must recognize the realities of the decentralized nature of responder procurement and the limited resources available. Compared to corporate product development or federal government acquisition, there are many more significant players in the process. The process must encompass a myriad of state and local agencies; strategic leverage in the process can be provided by Federal money, national standards, federal government and independent testing, and focused (and typically competitive) commercialization activities involving vendors of responder equipment.

Finally, to be maximally effective, new technologies and new operational procedures must be developed together, in an iterative process. For this reason, many of the technology plans described below include processes like the Defense Department's Advanced Concept Technology Demonstrations (ACTDs), which combine technology developers and operational users to integrate relatively mature technologies into innovative operational capabilities. Moreover, the rese arch and development process itself will provide new opportunities and prove others to be less promising than initially thought.

These technology plans, and the needs that underlie them, will not be the final word on responders' needs and capabilities. Capabilities and needs continually change, and the plan must evolve in response to new R&D results as well as to operational innovations. The goals and objectives of this and subsequent documents should be considered just that – goals, not threshold or exit criteria for capability development. As capabilities are built and fielded, this plan will change. As new threats emerge, needs will change, requiring further changes to the plan.

For all these reasons, this plan should be considered the first contribution in an iterative process to the continual improvement of responders' capabilities via an evolutionary development and deployment process that will work in the dispersed responder marketplace.

Contents

Chapter I

Introduction

Each National Terrorism Response Objective (NTRO) chapter below presents technology roadmaps made up of new initiatives to close gaps in responder capabilities. The building blocks for the roadmaps are Response Technology Objectives (RTOs), located at the end of each chapter. The RTOs recommend programs for the federal government to adopt (in addition to current efforts), and most are linked to the prioritized needs of emergency responders. The RTOs include descriptions of the objective and its goals, the payoffs that will result from the RTO, challenges that will be encountered while pursuing the RTO, and milestones and metrics by which developers can structure a program and gauge its progress. Each RTO also includes rough budget estimates. The following discussion describes the foundation and process used to link needs to technology, and derive these building-block RTOs.

A. Vision

The vision guiding the strategy to improve the capabilities of our emergency responders is:

> *Emergency responders should have the capability to prevent or mitigate terrorist use of chemical, biological, radiological, nuclear, or high explosive/incendiary (CBRNE) devices and emerging threats.*

In addition to the specifics of CBRNE devices and emerging threats, responders need to be prepared to deal with the catastrophic scale of effects that these threats may produce; thus a need for technologies to rapidly coordinate and integrate response capabilities from multiple local, regional, state, and federal organizations and disciplines is implicit in this vision.

Furthermore, although this vision and resultant plans envision response to catastrophic terrorism, technology development should aim, when possible, for increases in "all-hazards" capability. That is, technology development should improve responders' capabilities to deal with all types of catastrophes, whether man-made, natural, or accidental.

B. Strategy

Developing a technology plan to fill gaps in responder capability is important but it will not be enough by itself to actually increase emergency responder capability across the nation. This will be a new undertaking on the part of the federal government. Organizations responsible for improving responder readiness for catastrophic events need to develop a strategy for implementing the technology plan and assuring the successful transition of new technology into the hands of emergency responders. Those organizations should consider the lessons learned by other agencies who have managed similar activities. Some of those lessons are including in the following ten imperatives we believe should be included in such a strategy:

- *Establish and exploit appropriate responder collaborative environments* – Project Responder has established a network of responders, from all the emergency response disciplines in order to understand their needs as they themselves articulate them. The best way to assure that the products that result from the technology plans are useable by the constituents who need them is to continue to listen to them throughout the process. A broad-based representation of users (responders *et al.*) should be involved in the development process. The Integrated Project Team approach used in the DoD and other agencies may be a useful model, but making it work in the fragmented responder

universe will require significant adjustments and probably the regular use of distance-collaboration technologies.

- *Focus federal, industrial, and non-profit investment on the most pressing needs articulated by responders* – This plan offers a prioritized list of needs. This prioritization should continue to be explored with responders and those who are responsible for preparing the nation for terrorism to ensure that resources are applied to the highest priorities and payoffs. Influencing non-federal investment is crucial because of the decentralized nature of the responder community and the reliance on commercial vendors; these influence mechanisms need more attention and focus.

- *Insist on affordable end-products* – The Director of the Homeland Security Advanced Research Projects Agency recently said that affordability must be a performance specification for homeland security systems. State and local governments are and will always be resource limited. Responders buy their gear from commercial firms who must compete on price as well as technical performance. Affordability must be addressed at every step of the development process.

- *Leverage existing federal, state, and local government investment and infrastructure* – Governments have substantial preexisting investments in response capabilities—there is a large capital stock in use and responders are familiar with established operational patterns. Systems developed for use by local responders must take advantage of and integrate well with current equipment and infrastructure. Systems that require the wholesale replacement of existing equipment and infrastructure will be doomed to stay on the shelf because response agencies simply can't afford them.

- *Where possible, include terrorism response capability into upgrades of normal duty clothing and equipment* – Responders can not afford and do not want specialized terrorism response equipment. It is clear from our research that, where possible, the best way to increase our country's ability to respond to terrorism is to increase responders' ability to respond to all events—the so-called all hazards approach. While some capabilities will remain the province of specialized units, the *first* response will almost always be by non-specialized, front-line personnel with day-to-day equipment. The only way *first* responders will be equipped to deal with the situation is if the materiel is widely dispersed throughout the force. This approach also may achieve affordability through economies of scale.

- *Achieve continual improvement through spiral development and evolutionary deployment* – For reasons of affordability and interoperability, new responder capability will often need to be implemented through evolutionary upgrades of existing systems. Spiral development also offers the opportunity to maximize improvements by taking advantage of experience with the earlier deployed version of equipment. Costs are lower, too, compared to multiple new system developments.

- *Emphasize open architecture, interoperability, and proactive involvement in establishing appropriate standards and testing* – Open architectures are critical to being able to make evolutionary improvements in capability. This approach also lowers cost and increases performance by lowering barriers to entry into the market and creating more effective competition. Open architectures also help to define and enforce interoperability. Multiple jurisdictions and levels of government must be able to work together to respond to catastrophic terrorism. Current gaps in interoperability among their various systems have stymied that ability. Interoperability must be a absolute requirement for new systems. Standards and testing to those standards will be an important enabler of interoperability.

- *Identify existing commercial and government advanced technologies for integration into innovative solutions to meet responder needs* – A significant amount of technology that has the potential of dramatically increasing responder capability appears to be available in the

commercial world (primarily in the information technology industry) and in the federal government (especially in the Department of Defense). It has not yet been focused on responder needs. Leveraging this investment will enable early improvements in responder capability sooner and probably save money. Early investments should be made to adapt this technology for use by the responder community and to facilitate its adoption.

- *Quicken the maturation and deployment of advanced technology products, innovative concepts and eventual capabilities through modeling and simulation, demonstrations and effective commercialization* – Modeling and simulation (M&S) has proven to be a very useful tool in determining how systems will work together before they are built. Both the systems that are being considered, as well as the environment they will be operating in can be modeled in most cases. This allows the testing of how systems will work before committing to building expensive prototypes. M&S is also scalable so that new response concepts (the combination of new operational concepts with new technical capability) can be tested at the tactical unit level as well as the incident command, regional and even national levels. In combination with exercises and demonstrations, M&S can prevent or mitigate false starts, help assure that the systems will work in the intended environments, and help develop new concepts of operation that can increase the capability of new systems even before they are deployed. M&S will not obviate testing the actual systems. It can, however inform the trade-off process throughout the development process, saving money in the long run.

  Unlike the military, responders buy their equipment in the commercial marketplace and each local jurisdiction, for the most part, buys separately resulting in a highly fragmented market. Any technology developed by the federal government must eventually make its way to the responders via commercial vendors. Commercialization of government developed technology must be addressed from the beginning and throughout the development cycle. Commercial vendors should be involved at the earliest possible opportunity.

- *Focus investment in strategic research areas to provide future opportunities* – Although there appears to be a great deal of technology that can help responders available in the near-term, the solutions to some of the response community's most vexing problem are not on the horizon and the chance to develop leap-ahead capability must not be ignored. Therefore, any prudent R&D portfolio must include investment in fundamental research to solve those problems. We have recommended several areas where investment in basic and applied research is needed to provide the answers to needs across many responder capability areas.

In addition to these imperatives, a strategy to implement a successful responder R&D program should consider a few other elements beginning with how the R&D portfolio is managed. A dialog between opportunity and risk lies at the heart of any technology investment decision; where to invest along the risk continuum is a tough question. One must make "trade-offs" between the level of desired capability and the likely cost of and time to get to the eventual product. For all except the least risky, near-term investments, all R&D activities have learning at their core. Along the way discoveries will be made, unexpected obstacles may impede progress, and new knowledge may provide unexpectedly easy paths to improved capability. Although investment to reduce uncertainty is an important element of any well-planned R&D effort, it is impossible and imprudent to reduce overall risk to zero.

Therefore, at least some of all but the lowest-risk projects should be expected to fail. Some number parallel efforts (*e.g.*, different research paths to the same goal) should be pursued, even to the extent that projects might seem to be duplicative. Individual failures should be expected and should not be cause for indictment of the overall program. Sponsoring agencies must understand the need for flexibility as R&D goes forward.

In theory at least, planners should weigh the prospective value of any technology investment, discount this value by the assessed probability of success (technical risk), subtract any non-monetary costs and risks, and then divide by the projected R&D investment. This notional benefit/cost ratio would allow a comparison of "bang for the buck" across different proposed technology investments, providing an indication of how efficient the R&D program will be.

In practice, of course, such arithmetical exercises frequently fail to give a definitive indication because it is too hard to assess the projected benefits in numerical terms, and because it is hard to account for important second-order benefits of R&D. Moreover, the calculus needs to take into account the interaction among various projects. For example, the value of a four-hour protective suit would be limited if the mask that goes with it only protects for thirty minutes. While the NTRO chapters were prepared with this opportunity/risk calculus in mind, and the suggested investments were checked with a crude version of this calculus, expert judgment was viewed as superior to arithmetic in arriving at a coherent overall plan. Thus the technology effort must be viewed as an investment portfolio, in which opportunities and risks are balanced and spread across multiple projects.

One key to managing technical risk is to ensure that the level of integrated development does not get ahead of the maturity of the component and system technologies being integrated. Technology Readiness Levels (TRLs), developed originally by NASA and endorsed by the Defense Department, provide a systematic approach to this management process and should be considered for adoption by the Department of Homeland Security for its R&D activities. For example, no developmental technology should be slated for inclusion in a developmental system until it has had the equivalent of a successful "technology demonstration" (TD) that demonstrates the maturity of the technology and readiness to move to the next level of development.[3] A combination of component-oriented TRLs and system-oriented Integration Readiness Levels (IRLs) can be used to manage risk in complex development and integration programs. The readiness levels used by the DoD and others are described in Appendix A.

In addition to the risks of technology development, successful implementation of an R&D program has other risks as well. Technology development has its own equivalent of "the operation was successful but the patient died." Often an apparently successful technology development fails to find users because the specification was based on an inadequate understanding of user needs and operational context. Requirements for interoperability, user-friendliness, and cost are obvious examples of areas that need to be worked out in advance. In other words, the technology transfer process has important risks that must be assessed and managed in addition to the risks of technical development *per se*.

There are proven ways to manage and reduce these technology transfer risks. The Defense Department has been successful in its Advanced Concept Technology Demonstrations (ACTD), which integrate mature (and often commercially available) technologies and products in a novel operational concept to demonstrate the value of new capabilities or new technology-supported operational approaches. By involving users from the outset and producing a small "leave-behind" capability, the ACTD process focuses attention on real user needs and enforces attention to the real operational environment. This sort of mechanism is proposed in a number of the Responder Technology Objectives in the NTRO chapters.

Finally, creating a technology plan for improving capabilities to prevent and mitigate catastrophic terrorism is to some extent addressing the secondary needs of responders. In many areas, responders view their capability shortfalls as not being primarily solved by technology; resources and problems of integration across different governmental organizations are a more immediate concern. These vital responder concerns should be addressed by the United States Department of

[3] The Defense Department equivalent is the Advanced Technology Demonstration (ATD).

Homeland Security and other responsible government organizations. Although the plan does not speak directly to policy and financing issues it is nonetheless understood that they will play an important role in increasing the nation's capability to respond to terrorism.

C. Strategic Research Areas (SRAs)

Research in basic science and advanced technology offers the potential for leaps in capability. Investment planning tends to short-change these longer-term efforts because the pay-off is less certain than low-risk development projects using nearer-term technology. This is especially the case in an area as urgent as improving responder capabilities for catastrophic terrorism. An appropriate overall investment strategy should provide opportunities for investment in basic and early applied research relevant to the key problems and in promising approaches that are off the beaten track.

Five such areas are described below. They are strategic in three ways. First, they address technology development at the strategic level – that is, a long-term, risky commitment to developing solutions that are yet to be discovered, where success is only likely to be achieved beyond the timeline of near-term or existing technology solutions. In this sense, it also requires "strategic" funding, beyond the normal programmatic timeline of two to five years.

Second, they are strategic in impact: the resulting increase in capability from successful research will be more than incremental. Rather, successful strategic research will revolutionize responders' systems, giving responders a discontinuous improvement in capability.

Third, they are strategic in breadth. Although a Strategic Research Area may be central to a specific functional capability, successful research in these areas will benefit responders across many domains of capability and even across NTROs.

Many other areas of research—especially basic research—could also have been identified as important for dealing with catastrophic terrorism in the future. The areas identified here combine the promise of basic research with a more focused emphasis on responder needs.

Nanotechnology

Potential improvements in Personal Protection and Equipment motivated the definition of this SRA. However, its benefits, together with those of Surface Science (discussed immediately below), will also contribute to capability increases in Detection, Identification, and Assessment (DIDA.1 *On-Scene Detection*); Unified Incident Command Decision Support and Interoperable Communications (UIC.1 *Point Location and Identification*); and Response and Recovery (R&R.2 *Rapid Decontamination of High-Value and Critical Response Equipment,* R&R.6 *Specialized Search & Rescue,* and R&R.8 *Residual Hazards Assessment and Mitigation*).

Objectives:

Building structures at the molecular level to meet desired goals in the performance of materials for personal protection and equipment.

Thrusts:

- Creating fibers and cage structures,
- Characterizing them,
- Studying their performance vis-a-vis several of the goals in PPE.

Applications:

- Fabrics with improved and controllable permeability for uniforms.
- Fabrics with chemically reactive substituents for self-decontamination properties.
- Porous materials perhaps based on nanotubes or bucky-balls and capable of storing large quantities of air at modest pressures.

Surface Science:

Also central to capability increases in personal protective materials is strategic research and

development in the chemistry and physics of surfaces, especially modified surfaces.

Objectives:

Learn how to create and chemically modify surfaces to enhance material performance for personal protection goals.

Thrusts:

- Create materials with very high surface areas.
- Modify those surfaces chemically to provide reactivity with toxins, either stoichiometric or catalytic.
- Synthesize molecular cage or tube structures and evaluate their ability to absorb large volumes of air.

Applications:

- Self-decontaminating materials.
- Improved filter elements useful against all toxins.
- Storage of large volumes of air in SCBA breathing tanks at moderate pressures.

Observables and Sensing for Stand-off Inspection of Containers with Chemical or Biological Agents

The requirements of Detection, Identification, and Assessment merit a national-level strategic investment in research and development in this area. Strategic research and development in this area will also benefit numerous functional capabilities, described in other NTROs, that require indication or assessment of the presence of chemical or biological agents.

Objectives:

- Discovery and development of revolutionary approaches to rapid, non-intrusive stand-off detection and identification of chemical and biological agents in packages and containers, with effective ranges of a few feet in unconstrained geometry.

Thrusts:

- Candidate phenomenology and signatures.
- Theoretical detection and identification limits.
- Sensing concepts.
- Practical limitations and potential countermeasures.

Research should focus on those problems for which no potential solution is being considered, or for which a near-term solution does not seem possible. For example, the DoD is experimenting with contact sensing of chemical agents, with some good results; this research objective should look for phenomenology and concepts that do not require physical contact with the package. Such concepts may be extensions of current work to non-contact approaches as well as entirely new concepts and observables. Both active and passive sensing strategies should be studied: directed energy beams, optical, acoustic resonance, backscatter, and telltale residue detection should be considered.

Chemical agents in fluid state may have resonances that can be excited at short range by energy pulses or acoustic waves. Biological powders will pose the most serous and difficult threat since they may be shipped in very small quantities and may be in solid form. Based on current understanding, it is likely that some threats in the most difficult scenarios will not yield to a solution. The research program should identify the solution space for techniques developed, develop detection models, and define limits of performance. This will permit sensor developers to proceed in applications to provide useful devices for the responders.

Applications:

- Chemical and biological agents hidden in properly sealed containers and vessels pose a serious threat from terrorists. Such threats are impossible to detect with current technology; thus responders plan for detect-to-treat rather than detect-to-stop for CB attacks. Unlike

airport luggage screeners that force bags through a sensor system, responders may confront a nearly limitless variety of packages in unconstrained geometries. They may not have the time or access to more than one view or perspective, and the scenario may not be conducive to physical contact with containers. The discovery of new sensor phenomenology suited to this problem and the development of field sensors would provide a major tool in defeating CB attack before it occurs. Depending on the resultant sensor concepts, a wide variety of sensor types may be possible: handheld, suitcase, networked, automatic.

- Direct applications for the responder of this development would include on-scene analysis of suspicious packages, choke point screening of luggage and mail, screening of shipping and trucking containers, and warehouse and storage facility screening.

Ultra Wideband (UWB) Communications

Research in this field will support functional capabilities in Unified Incident Command Decision Support and Interoperable Communications, as well as functional capabilities in other NTROs that require communications or telemetry, especially through mass such as collapsed rubble or in areas where commercial wireless communications cannot function today.

Objectives:

Achieve communications penetration through walls, in high rise buildings and underground.

Thrusts:

- Improve characterization of radio frequency propagation through buildings and rubble.
- Develop understanding of theoretical limits of UWB performance.
- Characterize and bridge gaps between current and theoretical performance in prototype systems.

Applications:

- Point Location and Identification.
- Communications in areas that cannot be accommodated by wireless.
- Covert communications.
- Short-range, high-bandwidth wireless communications.

Biomarkers of Agent Induced Disease and Systemic Injury in Humans, Plant and Animals

This research area is central to Public Health Readiness for Biological Agent Events and Medical Response, and also to Mitigation and Restoration for Plant and Animal Resources. However, its benefits are also generally important to the Detection, Identification, and Assessment NTRO, and specifically to functional elements in several NTROs that require the identification and assessment of biological and chemical agents.

As a complex homeostatic system, the human body reacts in complex ways to insult. Focusing on the disease and trauma processes, and the body's responses to them, this Strategic Research Area will identify useable markers of exposure, disease and systemic injury. These markers can be used for screening individuals and making treatment decisions. Some of these markers of chemical or biological exposure or infection may be detectable without invasive sample collection.

Accurate assessment of chemical poisoning and physical injury or burns has benefits for triage in various contexts. In the case of physical injury and burns, one would hope to detect early stages of major organ failure that might not be obvious otherwise.

In the case of attack by an infectious agent which replicates in the body, the body provides its own culture medium and amplifying systems for detection and identification of agent. The sooner a biological attack can be detected and characterized and the victims identified, the better the

chances that a disease outbreak can be contained and that exposed individuals will survive. In many instances the threat agent will not be detected in the environment and the earliest possibility for detecting and characterizing the agent will be through testing specimens from exposed individuals. The hypothesis is that early stages of the disease process and the body's initial response to a pathogen produce measurable signatures that would be useful for early identification of exposed individuals and at least preliminary characterization of the agent. Such testing will also be useful to distinguish contagious individuals from those who are not dangerous to others.

Aside from its value in preparedness for a terrorist attack, this research has the potential to revolutionize the practice of internal medicine. Moreover, the required machinery and consumables are only likely to be effectively available in sufficient quantities (and with sufficient reliability) if they are in routine use in medical practice. Therefore this strategic research area should be conducted or at least overseen by an organization with broad medical responsibilities such as the National Institute of Allergy and Infectious Disease.

The benefits from research on plant and animal biomarkers are as significant in agriculture and animal husbandry. These fields are important to human health as well, because animals and plants can be vectors for human disease. The payoff in these fields would appear earlier because of the lower threshold for regulatory approvals for tests and assessments applied to animals.

Objectives:

- Developing knowledge of signatures of exposure, injury, poisoning, and disease process, and the body's response; understanding the availability of these signatures for sensing and for testing of specimens; and understanding how these signatures change during the course of chemical exposure or disease induced by biological agents.
- Assessing the usefulness of these indicators as discriminators between different threat agents and between the infected and non-infected states, and between severe and less severe injuries and illnesses.
- Understanding the value of alternative rapid clinical testing systems for accurately reading and assessing these indicators.
- Expand basic knowledge of plant and animal genomic structures and functional genomics.
- Characterize and assess biomarkers of plant and animal disease.
- Develop the substantive information underlying databases that can be provided to "first detectors" and emergency responders to discriminate between normal conditions of plant crops and other plants vs. the presence of contaminants or pathogens of concern in national agricultural defense.

Thrusts:

- Understanding biomarkers of exposure and disease progression in human and animal breath, saliva, mucous, sweat, blood, excreta, and retinal scans.
- Calibrating the wide range of "normal" values to be expected in humans, animals, and plants.
- Physiological markers and signatures of disease.
- Plant and animal genomic and proteomic variability and systems.
- Drawing conclusions from field observable physiological symptoms.
- Assessing the potential of methods of rapidly and reliably "reading" biomarkers.

Applications:

- Screening for injury or illness.
- Identification of disease agent.
- Distinguishing contagious from non-contagious individuals.

- Triage for agriculture, animal husbandry.
- Understanding of wild animal disease vectors.

D. Planning Process

Project Responder has identified key areas where additional investment in technology development and commercialization could provide high payoffs in response capability in both the near and longer terms. It has done this by involving responders and technologists in a disciplined process that takes current and emerging technologies and advanced products into account. Within these key areas, it has been able to suggest mechanisms by which these payoffs can be achieved.

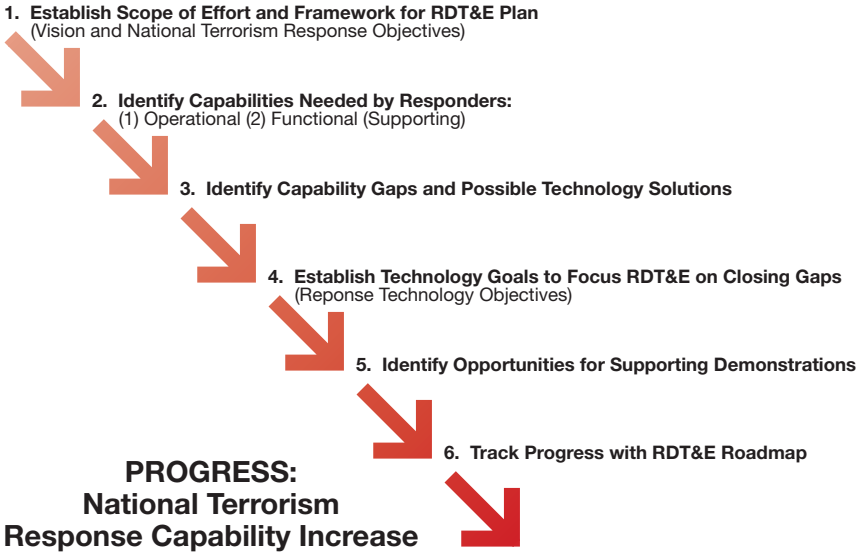
For example, one of the key capabilities of interest to responders is for squad, departmental, and incident commanders to be able know the position, and, if possible, health status and cumulative agent exposure status of all responders at an incident scene. Inexpensive radio-frequency technologies are available to perform at least the location function in open environments, but technologists are not sure how or even whether these capabilities could be provided within buildings, underground, or in the rubble that could result from a building collapse. The technology plan for unified incident command thus includes two thrusts in this area: first, evaluation of operational and system concepts that integrate current technologies and demonstration to facilitate commercialization of a near-term solution; and, second, strategic research into the propagation of Ultra Wideband Radio Frequency signals underground, in buildings, and in rubble, to precede the system design of a more capable, longer-term, solution.

The following chapters contain technology plans for the twelve National Terrorism Response Objectives (NTROs) identified by this nation's emergency responders as documented in the Project Responder March 2003 report. The twelve NTROs provide a structure whereby the breadth of emergency responder capabilities, required to successfully respond to a catastrophic terrorism event, can be divided into manageable pieces for the technology planning process.

These plans assume that, whereas emergency responders will have the responsibility to deploy and use equipment and technologies in response to terrorist acts, the federal government will have primary responsibility for investing in research and development of technologies for terrorism response not currently available and not under development commercially.

The technology plans result from a six-step process designed to develop a "capabilities-based" national technology plan for terrorism response. Although the steps in the process are depicted as sequential, in practice they overlap and were conducted iteratively. The steps in the process are depicted below.

Each NTRO chapter contains five elements: a definition of the needed capability, a set of *operational environments* for evaluating capability



Six-Step National Terrorism Response Technology Planning Process

needs and shortfalls, a number of *functional capabilities* that together define the operational need in more detail, a discussion of current capabilities and shortfalls for each of the functional capabilities, and the technology plan itself, made up of a summary technology roadmap and a set of Response Technology Objectives, structured to guide technology investments in order to produce a relatively efficient and orderly improvement in capabilities available to responders.

Operational Environments

Operational environments represent the variety of contexts in which the functional capabilities are assessed. The operational environments defined in this process have been deliberately kept broad and simple. There is infinite variation in the operational environments emergency responders may face. However, it was clear from the workshops that emergency responders automatically calibrate in their minds the type and magnitude of events about which they need to be concerned. Asking responders to work through detailed scenarios to arrive at requirements did not appear to improve the process and seemed in some instances to constrain thought by focusing too tightly on the details of the particular scenario presented. The responders were comfortable with the level of detail and variation the current structure provides. While this level of detail has been chosen to appropriately represent responder perspectives, it is possible that a higher level of discrimination will prove necessary in some specific cases as detailed technology planning proceeds.

Functional Capabilities

The functional capabilities represent the tasks or functions that must be accomplished in order to achieve mission success within the overall definition of the NTRO. If responders cannot currently accomplish these functional elements as they have defined them, then the elements include unmet needs—gaps that must be bridged if responders are to be prepared for terrorism.

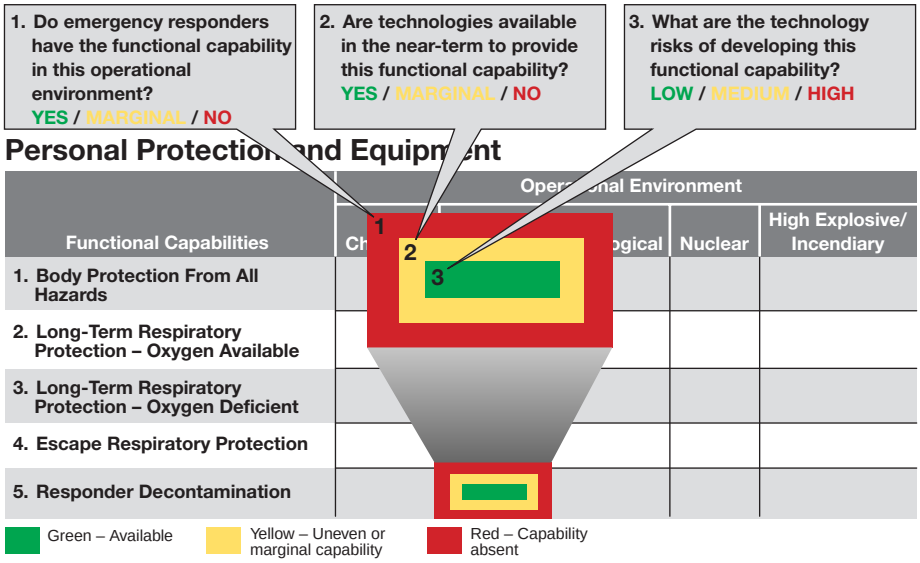
The functional elements in this document have been vetted in dozens of field interviews with responders and technologists at the local, state, and federal levels, reviewed by senior experts on the Senior Advisory Group, and further tested in depth and refined in eight workshops. These interviews and workshops reflect the expert insight and advice of over 125 emergency responders across all disciplines, and over 135 technologists and planning experts from government, laboratories, universities, and industry.

Within each NTRO, functional capabilities appear in order of priority (*i.e.*, importance as a needed response capability). In interviews and workshops, the responders were asked to prioritize among the marginal or unavailable capabilities: "which ones are most important to have soonest?" However, one must keep in mind that a response objective (*e.g.*, a NTRO) will not be met without some level of capability present from all of the functional elements. Moreover, the functional capabilities are defined at a sufficiently high level of generality that some needs in a high-priority functional capability may actually be less urgent than some of the most important needs in a lower-ranked functional capability.

Current Capabilities and Shortfalls

The analytical bridge between a statement of needs and a technology plan is an understanding of the gaps between capabilities available today and the prioritized goals of responders. To support this analysis, the operational environments and supporting functional capability elements are arrayed on a matrix, with operational environments along the horizontal axis and functional capability elements on the vertical axis. At each intersection in the matrices, three nested boxes appear, with each box colored either green, yellow, or red. The colors within each nested box indicate the availability of capabilities and technologies, as illustrated in the sample chart on the next page.

The color of the outermost box indicates the availability of the functional capability to the responder. That is, for this box, the Project asked participants "does this functional capability exist today for the operational environment?" The



Sample NTRO with Color-Coding Legend[4]

results of that assessment are expressed in the matrices by assigning a color to the outermost box: green if the functional capability exists today; yellow if the capability is marginal or unevenly available among responders; and red if the functional capability does not yet exist.

If the availability of a functional capability element was judged to be limited or non-existent, participants were asked to consider why this is so (*e.g.*, is it a cost issue for all or some jurisdictions, or is the technology just not there?). The responses to that question are noted in the discussion of the Current Capabilities for each functional capability element.

For functional capabilities where the responders indicated marginal or no availability, Project Responder brought together technologists and responders in workshops to recommend technology programs to close those gaps. To lay the foundation for these recommended programs, the NTRO chapters summarize existing technology programs and areas of development that have application to the functional element, and characterize what technology limitations and barriers are in the way of achieving the needed capability.

The NTRO chapters also summarize "Gap Fillers." The discussion in these sections generally describes technology and non-technology measures that could be taken to close the gaps between what responders need and what they have. Where specific technology development programs are recommended, the Gap Fillers are more fully described at the end of the chapter, in the Response Technology Objectives. However, the Gap Filler discussion also includes some options for technology transfer that can improve capability without a development program, as well as non-material solutions (*e.g.*, changes or increases in funding for training, doctrine, organization, etc.).

Based on this information, the project asked the technologists and responders "what is the near-term availability of the technologies needed to fill the gaps in capability?" The answer to this question provides the color for the second nested box in each matrix cell. The box is green if technology is available in the near-term (*i.e.*, less than five years). The box is yellow if technology is marginally available in the near-term. The box is red if technology does not seem to be in the R&D pipeline.

Technologists were asked to assess the overall technological risk of the R&D effort required to surmount the gaps identified. This level of risk is represented by the color of the third, innermost nested box in each matrix cell. For this issue, technologists were asked "what is the technological risk for developing technology to close these gaps?" The box is colored green if the risk was considered low, yellow if the risk was considered

[4] Note that if an outer box is green, the subsequent issues are irrelevant and thus not addressed. Thus, areas where capability is available would be represented by a single green box. Furthermore, if a box is gray, responders believed that the functional capability was not applicable to that specific operational environment.

moderate and red if the risk was considered high. Because of the level of aggregation at which these judgments were made, they must be treated as an overall characterization of the technical difficulty of achieving all of the responders' goals, rather than the level of technical risk associated either with each goal.

One purpose for providing these data points in a simplified color-coding schema is so that readers interested in the forest more than the trees can easily orient themselves to the overall pattern of gaps in capability and the likely role of current and additional technology investments in bridging these gaps. Thus, towards the beginning of each NTRO chapter below, the entire NTRO and its constituent functional capabilities are represented in a single matrix with the color-coded boxes. This matrix helps the reader identify at a glance three important facts: those areas where improved capabilities are needed, the degree of focus and likely success of existing technology programs in providing the full set of capabilities wanted by responders, and the significance of the technological obstacles that stand in the way of delivering those capabilities.

Areas with red in the outer boxes (that is, with severe shortfalls in capability available to emergency responders) but with a green middle box are areas where existing technology programs will provide solutions, or in some instances where the needed solutions are primarily not technological in nature. (The needed solutions may be organizational or budgetary.)

If the middle box is red or yellow but the innermost box is green, that means that current programs are not adequately focused on responder needs but that low-risk technology solutions are available. In this case the appropriate recommendation is for a technology integration (low-risk development) program or even simply a program for encouraging the commercial integration of commercial-off-the-shelf technology (COTS) through a testing and certification program. On the other hand, matrix cells that are all red represent a needed functional capability element that poses significant technological challenges to achieve the *ultimate* desired level of capability. For some capabilities, it will be important to pursue *both* near-term and longer-term development efforts, with some attention to transition between the two, to maximize important responder capabilities in all time periods.

Technology Roadmaps – Goals to Close Capability Gaps

Each of the NTRO chapters presents technology roadmaps that describe the development path to greater capability. The building blocks for the roadmaps are Response Technology Objectives (RTOs). The RTOs represent recommended programs for the federal government to adopt, in addition to current efforts. For some needed functional capabilities, it is natural to define a coherent technology effort to remedy all the technologically-determined capability shortfalls in a single program. In these cases, there will be a one-to-one mapping between the RTOs and functional capabilities. In other instances, key technologies may enable more than one functional capability, or a functional capability may require a heterogeneous set of technologies to fill the identified shortfalls.

As presented in the NTRO matrices, the assessed level of technological risk in meeting key capability objectives plays a key role in determining what sort of technology effort is proposed. High technological risk generally implies a need for applied or even basic research to develop information about the feasibility of novel technical approaches. A high degree of parallelism in development would also be desirable. An intermediate level of risk suggests that the basic technical knowledge is available but that the implementation of this knowledge pushes the current state of the art, requiring a significant engineering development effort.

Low technological risk implies that the shortfall can be remedied through straightforward combinations of known technologies that are already available in the military or commercial spheres, whether they are already combined in commercial-off-the-shelf products or not. Low

technological risk should not be taken to indicate that little effort or ingenuity is required; the combination of significant unmet needs and low assessed technological risk often suggests the presence of thorny technology integration issues (for example between multiple existing and novel systems) or significant organizational roadblocks to technology adoption; effort required in these instances may in fact exceed that needed to develop some previously unavailable widget that on its own solves a capability problem.

In some functional capability areas, improved capability is urgently needed yet the ultimate technological solutions require extensive research and development. This situation generally prompted technologists to recommend a multi-pronged approach in which a relatively low-risk development program can be aimed at a set of meaningful intermediate capability goals while higher-risk and longer-term activities are begun that are oriented toward the ultimate levels of capability desired.

There is considerable art in defining technology objectives to close capability gaps. One wants objectives and interim milestones that are concrete enough to enable easy assessment of progress, but that are broad and flexible enough so that technology development programs can take advantage of learning during the R&D process. R&D programs with similar content need to be managed together, so that cross-fertilization is easy and so that budgets can adapt as some paths become more or less promising than originally thought. Thus the structure of the RTOs may need to be adjusted to the organization that ends up responsible for their execution.

The RTOs describe technology objectives and milestones, and provide rough estimates of cost and schedule. The cost and schedule estimates assume the continuation of currently programmed efforts in related areas and assume effective leveraging of those programs. The estimates are based on top-down expert judgment rather than a detailed bottom-up plan. More precise estimates would require knowledge of the actual budgetary and institutional environment in which the work is to be carried forward. Thus, the next step would be to choose a responsible federal agency and an execution strategy for each RTO, and determine the appropriate degree of risk and parallel development for each program, as well as the institutional context in which various research and development tasks would be performed. Even with this context firmly established, several planning iterations will be required to achieve stable and accurate cost and schedule estimates.

Because of the current rapid rate of evolution in the federal government's mechanisms for conducting homeland security R&D, the Response Technology Objectives do not identify specific agencies for program execution. However, the discussion in each chapter identifies some agencies that are participating in key areas of technology development: in such cases, it is important that current programs and expertise be leveraged in whatever new arrangements are developed in the Department of Homeland Security.

Chapter II

Personal Protection and Equipment (PPE)

Chapter Chair: Dr. John Lyons
Chapter Coordinator: Michelle Royal

Definition

Personal Protection and Equipment (PPE) is the capability to protect responders, via gear from the effects of chemical, biological, and radiological agents as well as blast and incendiary effects.

Operational Environments

The capabilities required of emergency responders and the needed protections will vary by the type of incident. Chemical, biological, nuclear, radiological, and explosive/incendiary events place different requirements on protective equipment. Within these distinct operational environments, there is a near infinite number of variations in terms of size, severity, specific agent, geographic area, and so on. However, responders believe that they need to be prepared for the full range of effects, and that these variations would mean little in terms of the protection they would need. Thus the discussion here deals largely with the four major types of threat agent that responders needed to be protected from: chemical, biological, radiological, and the heat and kinetic insult from explosive/incendiary events. The assessments in the tables are at this level. (The effects of nuclear explosions were resolved into combinations of explosive, incendiary, and radiological effects.)

In discussing Personal Protection and Equipment, responders have typically focused primarily on scenarios that can be handled locally; there has not been much discussion of nuclear holocausts, for example. Disasters involving large parts of states or regions, as would be the case for aerial dispersion of chem/bio agents, have not been discussed much, although such scenarios loom large at the national level. The responders in discussing Personal Protection and Equipment have stayed "close to their home turf." Nonetheless, responders believe that large events would affect the *amount* of protective gear needed, more than the *nature* of the gear needed.

Chemical and biological incidents are in between a strictly local problem and a national-level catastrophe – partly because of relatively common HAZMAT incidents; partly because of the special teams being formed at the national level, as well as recent anthrax incidents.

It should be noted that the responders want to minimize the number of sets of protective gear required. Therefore they want any proposed set of new gear to be effective, not only for the major terrorist disasters, but also for everyday events. (This means that the new gear must have all the different new features thoroughly integrated in the design.) This is not just a matter of limiting inventory or even saving time in turning out for an incident, although these are also very important. Many responders will arrive on an incident scene, often equipped only with everyday garments, before the incident has been fully characterized; in addition, there is a danger that terrorists will employ secondary devices at an incident scene that could add additional hazards to an ongoing incident. For these reasons, moving in the direction of an all-hazard protection capability will sometimes be a matter of life and death, not just convenience.

Needed Functional Capabilities and Priorities

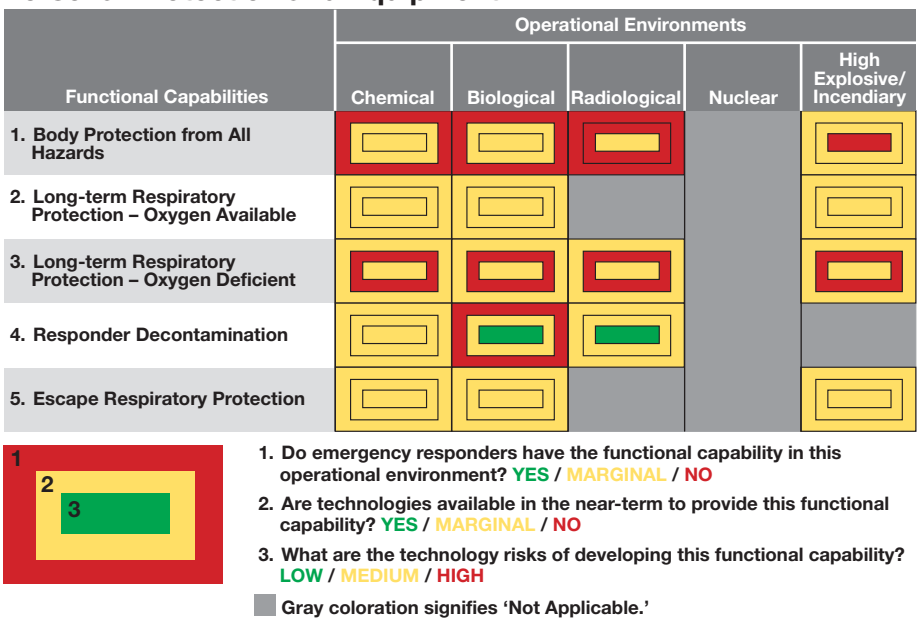
Protecting emergency responders is a top priority; keeping them in the best physical and mental condition is essential to maintain the vital

services they must provide. This NTRO is focused on gear such as clothing and masks for the individual.

Responders and technologists considered a set of five functional capabilities to handle the operational context described above. These capabilities are presented below in order of priority:

- Body Protection from All Hazards
- Long-Term Respiratory Protection – O^2 Available
- Long-Term Respiratory Protection – O^2 Deficient
- Responder Decontamination
- Escape Respiratory Protection

Personal Protection and Equipment



Responders' top priority is protecting the body, primarily through protecting the skin (*i.e.*, ranging from firefighter turnout suits to the full protection of HAZMAT uniforms) and then, protecting the lungs (*i.e.*, masks of various kinds). The discussion did not deal with preventing falls and other physical injuries.

Finally, the responders are concerned about the thoroughness of decontamination. This became part of the separate functional capability on decontamination in this NTRO, and also part of the sensor plan presented in Chapter III (DIDA).

Overall State of Technology for Personal Protection

The matrix to the right shows a mix of moderate to high technological challenges in raising the level of capabilities for emergency response. The chart shows relatively few green assessments, mainly for decontamination for radiological and high-explosive/incendiary, where responders feel they have acceptable procedures. The key technology challenges will be in body and respiratory protection, where (especially in respiratory protection) little research is going on and the trade-offs between weight and duration will be difficult.

PPE.1 – Body Protection from All Hazards.

The ability to have full-body protection for responders from all hazards: not only CBRE, but also toxic industrial chemicals and other hazardous materials.

This element includes not only terrorists' use of CBRE but also industrial chemicals and other hazardous materials. The rationale is that responders need to minimize the number of different suits, masks, and the like they must carry. This makes a one-suit-fits-all-needs solution very attractive. In this way the same protective system works for everyday hazards as well as terrorist disasters. As mentioned above, given the likelihood that responders will arrive at an incident before it is fully characterized, and the possibility of secondary devices with additional threat agents aimed at responders, the all-hazards suit will be a lifesaver as well as a convenience.

Goals:

The responders set the following goals for this element. These goals were used to assess the

current capabilities and provide the target capabilities for the plan.

- Lightweight: <15 lbs for the full ensemble (gloves, boots, suit, helmet) but not including add-ons such as microclimate cooling or communications gear – current bunker gear for firefighters is heavy when dry, and worse when wet.
- Rapid donning and doffing. Velcro has improved this a lot but donning essentially airtight gear against hostile atmospheres generally requires a second person to assist.
- Comfortable; microclimate conditioning – the airtight, watertight suits need climate control and ventilation for any extended period. It is likely that semi-permeable fabrics will require this too.
- Capable of being used with existing gear. If new items are to be used with existing items, old and new must be compatible. For law enforcement, the new suit must have a pocket for ballistic vests, etc.
- Improved dexterity, especially for gloves.
- Waterproof.
- Able to self-decontaminate – this suggests reactive chemicals in the material that will neutralize the hostile agents.
- Exceeds current standards. Capable of meeting anticipated future standards as they are produced and adopted.
- Built-in extraction handle. This will enable one responder to pull another out of a tight spot without taking off protective gear.
- Non-conductive electrically.
- A base suit that works for all missions with appropriate add-ons for different situations. This is a great challenge with a great cost payoff as well as simplifying logistics.
- Variable visibility of suits. Most of the time responders want to be visible but SWAT teams may want to have low visibility.
- Provide protection against thermal, ballistic, CBRE. These are the basic needs.
- Durable against tearing, puncture, and impact.
- Designed to fit. One-size-fits-all is not good enough.
- Hearing protection.
- Laser vision protection. Law enforcement officers, often first on the scene, are concerned about encountering terrorists using laser weapons.

Current Capabilities:

There are no ensembles that meet all of these goals. HAZMAT and bomb squad gear come the closest. Bunker gear for firefighters is heavy, becomes waterlogged, and is not designed for chem/bio or radiological hazards. It does a good job against thermal, impact and puncture threats. The military have suits designed primarily for chemical attack (though it turns out they are effective against biological attack as well). The Army has bomb fragmentation shields that are put under their uniforms, but they are heavy and cannot be worn routinely. The Army's battle dress overgarment and the Joint Services Lightweight Integrated Suit Technology (JSLIST) are both based on a charcoal interlayer to absorb the toxic agents. The JSLIST suit is a newer design, lighter and is claimed to be more comfortable.

Law enforcement officers have ballistic protection and little else. Emergency medical personnel currently do not make much use of special gear.

Radioactive sources may emit various kinds of injurious radiation. Some are either non-defensible with lightweight materials (gamma, neutron, and x-rays,) or they are charged particles with limited ability to penetrate the

skin or clothing (alphas, betas). The alphas and betas can attach to larger dust particles and find their way into the lungs or through breaks in the skin into the blood stream. Ingestion sometimes is possible. However the usual chemical suits provide excellent protection and the particles are easily washed off.[5] While exposure to known, low levels of gamma, x-ray, or neutron radiation can be limited by time to relatively safe levels, high levels require very dense metals such as lead for effective shielding. Specialized suits and, preferably, robots should be used for clean up and for insertion of high-level radiation sources into a shielded container.

All of the goals are desirable but most important among them are: lightweight protection, durable against tearing, puncture, and impact, good fit to the wearer, improved glove dexterity, waterproof, and compatible with other gear used by the service. The concept of a single base suit for all with add-ons for particular scenarios has great appeal but is regarded as very difficult technically to achieve. Cost savings from having one suit rather than many different suits would be substantial. There has, as yet, been no movement toward this goal. A possible exception is in the military as exemplified by the Army's work on semi-permeable fabrics. They are designed for chem/bio use; they may or may not be suitable for firefighting.

State of the Art:

There is a new research alliance at the Institute for Soldier Nanotechnology (ISN) at MIT that is conducting a basic and early applied research program covering some of the goals of this functional capability. Other efforts are underway at the Army's Natick laboratories. The focus of the Army's FFW program is similar to other goals of this functional capability.

At the Army's Natick laboratories, the focus is shifting from layered suits with a charcoal interlayer to a lighter suit with controlled or semi-permeable fabric. There is just enough permeability to allow water molecules to pass through (*i.e.*, sweat) but nothing larger. This concept is in late applied research wherein additional polymers are being evaluated. Whereas the current Land Warrior program in the Army is based on the JSLIST technology, the semi-permeable membrane technology is planned to come to fruition by 2010. The Future Force Warrior effort (fielded by 2015-2020 with the first units deployed by 2010) is planned to rely on semi-permeable fabric composites with active, self-decontaminating properties.

The DoD is supporting a significant university research effort to see what new benefits may be achieved through the use of nanomaterials and nanotechnology (see additional discussion of these technologies in Chapter I (Introduction) as (Strategic Research Areas)).

Technology Limitations and Barriers:

The challenge is not so much in designing a system to meet one or another goal but rather to meet all the priority goals in one system. Reducing weight will be a challenge. Power sources for cooling the suit will be a limiting factor as it is in nearly all military applications for the individual war-fighter. A particular challenge is providing seals at zippers and other closures.

There are many schemes with good performance against one or several hazards but they are not lightweight, easy to use, comfortable, or they fall short of other needs and goals described above. Resistance to chem/bio agents might be achieved by reactive agents in the material and by reduced or near-zero permeability. The effectiveness of reactive agents needs to be tested carefully to determine how much toxin specific fabric coatings can handle; to see if there is a possibility, or even a necessity, of a catalytic effect rather than a stoichiometric one; what the shelf life of the coating will be, and how responders can know if the active agent(s) are still active. These properties will not necessarily be useful in firefighting – and may be degraded by heat and water encountered in typical firefighting situations.

[5] See "Medical Management of Radiobiological Casualties Handbook" Armed Forces Radiobiology Research Institute, Bethesda, MD (April 2003).

What is needed is a combination of the latest in materials science and system engineering and ergonomics. The one-suit-meets-all goal is the most intriguing idea. Reaching agreement among the various groups of responders will be difficult and will require patience and skill in consensus building. This skill will be required both in defining performance requirements and in developing the necessary purchase standards when the technical barriers have been overcome.

All scenarios are rated yellow for adequacy of current technical programs. They have small budgets, the market is relatively small, and the test and certification capability is not adequate.

Gap Fillers:

The degree of risk for delivering these capabilities depends upon how ambitious the future R&D program objectives will be. For the one-suit-meets-all goals, the risks are very high. This is a stretch goal that may very well not be met in the early years but the fallout along the way should meet many of the goals. The chem/bio risks are moderate given the military's high priorities. Radiological risks are low for alpha and beta particles but high for gammas, x-rays, and neutrons. Ordinary protective garments will not address the latter three forms of radiation hazards. The risks for R&D on the high explosives and incendiary scenario are rated high because this is where the normal hazards of fire fighting, HAZMAT, and EMS fall along with the WMD high explosives and incendiaries. Most of the current federal R&D is aimed at chem/bio hazards.

The priority goals for protective garments are: reduced weight for the thermal barriers, resistance to tearing, puncture and impact, comfort, ability to breathe, suppleness, self-decontamination, cooling systems and power sources, and provision for integrated communications. The basic suit should contain as many of these as possible. However it is reasonable to mount separate research programs on some of these goals and then integrate the various pieces into a final product.

National nanotechnology research programs should be integrated into an overall plan so that results flow smoothly into the overall program outlined below. Integration of all the pieces must be planned. The acquisition strategy should be to involve all relevant research entities from the outset by forming integrated advisory bodies made up of suppliers, R&D activities, the ultimate fielding entity, and the users. Similarly, R&D alliances should be formed among the performers. This way the work can be kept on track and optimized easily.

The overall program might look like this:

- A basic and exploratory effort on self-decontamination, cooling systems and power sources, and sealing zippers and closures.
- An applied research program on fabrics to combine resistance for all scenarios using the various schemes now either commercial or in advanced development as starting points (*i.e.*, semi-permeable fabrics, products of nanotechnology research programs, and cooling systems on the military drawing boards).
- Development work to build prototypes first of individual technologies for separate goals and then of integrated systems; evaluate in the laboratory and in the field.
- Cost reduction via developmental engineering work to adapt military technology for emergency responder products.

PPE.2 – Long-Term Respiratory Protection Where Oxygen is Available (i.e., Air Purification). *The ability to have long-term respiratory protection in an oxygen-available environment (air purification).*

Goals:

- Duration: >12 hours.
- Weight: <10 ounces.
- Very low breathing resistance (400 liters/min. peak inhalation rate) and with positive pressure.

- Comfortable especially for the prolonged use anticipated in these goals.
- Vision – Full peripheral field of view (>120 degrees) to include both lateral and vertical. No fogging.
- Integrated communications capability to include back to incident command center and to other responders.
- Residual life indicators for expendable components.
- Affordable: <$300 each.
- Interchangeable components with other manufacturers' models.
- Capable of handling all hazards.
- Exceeds current standards and meets anticipated new standards as they are adopted.
- Resistance to heat and cold and flash protection.
- Serviceable at the home base as opposed to having to return to the manufacturer.
- Useful for health care providers as well.
- Low physical profile; non-snagging.

Current Capabilities:

The responders would like to have a single system with interchangeable components such as filters, face pieces, etc. The components should be interchangeable with systems from all manufacturers. This is not the case today but some of the goals are met by currently available systems. This functional capability is rated today as overall marginal and much work will be necessary to meet the all-in-one goal. There are different filters for different threats raising the possibility of the user selecting the wrong one, an action that could be fatal. Breathing resistance is too high, making the user work too hard to breathe and shortening the length of time the user can wear the gear. Communications are difficult, if not impossible, lenses fog easily and the equipment is too heavy. The manufacturer must service most current systems.

State of the Art:

There are programs under way addressing some of the goals but not in an integrated fashion.

Technology Limitations and Barriers:

The most difficult challenge is to reduce weight substantially while increasing the capacity of the sorbents. (The current capability is that it requires 11 oz. of sorbent to achieve six hours of protection.) Improved sorbents will help, but this is likely going to be a trade-off in design. Improved communication through the mask is very important and will be a challenge both technically and to the weight limitation.

The risks for most of the goals are not high; an exception is the weight-capacity trade-off. Solving this trade-off satisfactorily will require a breakthrough in materials and in design.

Gap Fillers:

The following kinds of R&D are needed: materials research; design of the mask assembly; design and performance of the filter elements.

- The materials work includes the sorbents themselves and should include new sorbents; *e.g.*, nanoparticles based on carbon nanotubes with additional molecules inside – caged structures – with a very high capacity. Current R&D results should be integrated with these projects.
- Additional material work should be devoted to lens materials, antifogging technologies, lighter weight mask materials and improved sealants.
- Construction and evaluation of performance should include various combinations of filter elements with the goal of increasing capacity per unit weight and thereby lengthening time in service; also layering in various combinations to achieve performance against the broadest possible spectrum of toxins. Reduced resistance to breathing is a must, and will be achieved from both new filter materials and designs; possibly some form of the power-assisted air purifier respirators might supply an answer.

PPE.3 – Long-Term Respiratory Protection in an Oxygen-Deficient Environment. *The ability to have long-term respiratory protection in an oxygen-deprived environment with unknown hazards.*

Goals:

- Long-term: >4 hours under stress.
- Heads-up display capability.
- Weight except mask: <10 lbs. (Current is 20 lbs without the mask.)
- Integrated communications to command center and other responders.
- Comfortable, ergonomically designed.
- Fragmentation/shrapnel/crush protection.
- Status indicator for consumable parts.
- Ability to withstand thermal loads, both hot and cold.
- Serviceable at the responders' home bases.
- Durable.
- Affordable: <$3000 each. (Currently $5000-6000.)
- Integrated environmental monitoring (addressed in Chapter III (DIDA), under "sensors").
- Full peripheral field of view, 120 degrees both lateral and vertical. No fogging.
- Integrated personal alert device to indicate distress emergency.
- Interchangeable components (especially the face piece) with other breathing apparatus.
- Meets appropriate and anticipated emerging future standards.
- Low physical profile; no snagging.

Current Capability:

Current systems include principally self-contained breathing apparatus (SCBA). Today's SCBAs are typically rated up to one-hour service at 4500 psi in the tank. They cost between $5,000 and $6,000 (*cf* the goals of four hours and $3000). The responders discussed rebreathers – systems that remove carbon dioxide and generate fresh oxygen. These were pioneered by the Navy submarine rescue programs and are used for deep-sea diving even today. They were used by fire departments (based on potassium superoxide, a hazardous material) before the newer, lighter weight SCBAs were introduced. Given that many years have passed and much new chemistry has appeared, it would be worth an R&D investment to see what new concepts may be possible. Tethered systems are not being addressed because of the entanglement problem. There is a new system available that claims utility as a rebreather for up to four hours. The maker also claims it has the potential to be adapted as a one-hour SCBA. It weighs somewhat more than the current SCBAs.

The SCBAs of today are heavy and have a nameplate lifetime of up to one hour. In practice, the wearer can only stay in the hazardous atmosphere about twenty minutes because of the need for ingress and egress time plus a good safety margin. This is enough time for a rescue but little working time otherwise.

State of the Art:

There is not much cutting-edge activity in this area. There is some new work on rebreathers in the Navy. The current posture was given by the Boston FD; namely, they abandoned rebreathers in 1978 when the improved SCBAs became available.

Technology Limitations and Barriers:

Reducing weight to reach the above goals while increasing duration of service is another difficult trade-off, similar to that for filter masks. The current fiberglass-wound aluminum tank was

developed by NASA thirty years ago. In the future there may be materials developments that permit higher air pressures. Alternative means of storing the gas (air) can possibly be had by novel sorbents within the tank to obviate the need for high pressures.

Other challenges for the masks are similar to those for filter masks.

The technological risks of achieving these goals are significant. Achieving much higher pressures in the air tank will be difficult and would require substantial advances in strength of materials. On the other hand, developing a solid sorbent system to hold large quantities of sorbed air would require both very different sorbents for air, and a system to release the sorbed gas. These are new departures and have inherent development risks.

Gap Fillers:

The R&D for the mask itself will be similar to that for filter masks (PPE.2 (*Long-Term Respiratory Protection – O_2 Available*)). There is a need for electronic communication from within the mask. The communication piece is a function described in Chapter IV, as an element of the Unified Incident Command Decision Support and Interoperable Communications (UIC) NTRO, but the integration of microphones, headphones, or speakers and controls and displays into protective equipment will need to be done as the suits and masks are developed. The same is true for power supplies for systems in the mask or garments, which are a part of Chapter IX (Logistics Support).

The air supply requires substantial exploratory and applied research to address the weight and duration goals. The assumption is that we cannot simply increase the pressures in the existing or similar tank systems to reach greater than 4 hours lifetime in service use and a weight for the storage system of under 10 lbs. What is needed is a low-pressure tank filled with a new air sorbent that will hold the requisite air weight in a modest volume at a modest pressure. This requirement is similar to that faced by the hydrogen-fueled car engineers, only much less hazardous.

PPE.4 – Responder Decontamination. The ability to decontaminate response personnel, including law enforcement and medical personnel, and their personal equipment on scene and in all weather conditions.

Goals:

- Environmentally benign.
- Benign to equipment.
- On-scene real-time detection of any residual hazards – decontamination assurance.
- Dry decontamination.
- Speed – fast as a baggage conveyor.
- Ability of the garments and personal equipment to self-decontaminate.

Current Capability:

Most methods in use today begin with drenching water showers. If chemicals or biological agents are suspected then the most common reagent is chlorine as solutions of sodium hypochlorite (common laundry bleach) in concentrated or dilute forms. These solutions are relatively slow – fifteen minutes exposure is recommended to destroy some biologicals; *e.g.*, anthrax spores. The concentrated form (5% – 6% for laundry bleach) is hazardous to the skin and eyes and should be used with caution.

A Canadian company has developed a foamed product that is said to be effective in bomb suppression as well as in decontamination applications.

The Armed Forces Radiobiology Research Institute has issued a report that states that decontaminating particulates containing alpha or beta particles (the only long-lived radiation hazards) is not difficult and the present techniques should be adequate – the particles are readily washed away. (Decontamination of wounds is somewhat more complicated.) In addition radiacs or geiger counters are effective sensors for residual radiation hazards.

Responders lack reliable sensors to determine whether chem/bio decontamination has been effective. They therefore are reluctant to reuse decontaminated garments. They prefer to discard them. There is a serious psychological barrier to reuse. (Responders are less wary of decontaminated solid surfaces; *e.g.*, tools and the like. See Chapter V (Response and Recovery).)

State of the Art:

There are two approaches at present: improved decontamination chemicals for use in showers etc., and self-decontaminating fabrics wherein reactive entities are built into the fabric. This is a relatively untested concept (see discussion under PPE.1 (*Body Protection From All Hazards*)) now in research funded by DoD. Chlorine-containing washes are hard on the environment and on the fibers. Substitute chemicals are being studied. The Army's Edgewood Arsenal has several projects under way including enzymatic decontamination, ultraviolet light decontamination for biologics, and high-pressure steam or even supercritical steam. There is no R&D on the psychological problem of reusing contaminated equipment such as garments. Sensors responsive at low concentrations on surfaces are required but not yet available. (See Chapter III (DIDA) for sensor development.)

Technology Limitations and Barriers:

There are two primary challenges: chem/bio sensors effective at low levels of surface contamination, and the psychological resistance to reuse of decontaminated garments. (See discussion above.)

The technological risk of developing these capabilities is moderate to low. There are a number of possibilities for destroying chemical or biological residues, and one can be optimistic that improvements over straight chlorine systems will be fielded. On the other hand, developing the low-level sensors capable of relieving the psychological barriers to reuse will be much more difficult. Given the concern over contamination from terrorist acts, the sensors are likely to be developed. Successful research into the psychology of emergency responders is more problematic.

Gap Fillers:

The several decontamination efforts currently underway should be coordinated and new funding for research coupled to these efforts. Current funding sources should continue their sponsorship. The self-decontaminating fabric concept is a good one; it is currently being looked into by the military. DoD is also looking at nano-fabrics engineered to detect as well as neutralize hazardous chemicals and biologics. Reliable sensors will be required to assure that the agents in the fabric have done their job. (See Chapter III (DIDA).)

Beyond maintaining or enhancing current R&D programs, the principal needs here are coordination and integration followed by field testing. Of concern is the completeness of the destruction of the toxins; this in turn means introduction of analytical techniques and sensors effective at detecting very low levels of toxins. Testing will involve trials with individuals in full field uniform exposed to a surrogate chemical, followed by a standard decontamination wash and then evaluation.

PPE.5 – Escape Respiratory Protection.

Protection for escape from contaminated areas but not used for entry and rescue operations.

Goals:

- Duration – 15 minutes.
- Easily deployed with safe packaging.
- Easily portable – on belt or in vehicle.
- Compact size: 4" by 3" by 1/2"; weight: 8 ounces.
- Extended shelf life – minimum five years.
- Lens – full peripheral vision (lateral and vertical) 120 degrees; no fogging.
- Nondegradable, environmentally stable; ruggedized.
- Disposable.

- Carrying case (designed to wear on the belt).
- All hazards.
- Status indicator.
- Resistant to thermal loads (hot and cold) and flash protection.
- Affordable (<$100).
- Integrated communications.

Current Capability:

The utility of the escape mask is to enhance the likelihood of escape from hazardous areas, not to perform tasks. Capability is marginal for rescue masks. They are not universally used, many in current fire service stocks are years past the expiration dates. Available products are not convenient to wear, need to be more compact, and are deficient in the same ways as air filtration masks (see PPE.2 (*Long-Term Respiratory Protection – O_2 Available*)). They are being distributed in some venues – the Pentagon recently distributed some 20,000 commercial products within the building. The Department of Defense Technical Support Working Group (TSWG) has recently had several hoods evaluated using a draft NIOSH standard. Large numbers of these have been purchased recently by the Departments of State and Defense. The Interagency Board for Equipment Standardization and Interoperability (IAB) urges more priority and funding for these masks. The IAB's requirements are similar to the goals listed above. Given that the fire service is more likely to require SCBAs in such environments, the users will tend to be law enforcement and the EMS plus civilians in certain venues.

State of the Art:

Some R&D is being done in industry; little in the military. The effort is probably sub-critical to achieving the goals described above.

Technology Limitations and Barriers:

Meeting the weight, size and duration goals will require a difficult trade-off. The result should fit on the responder's belt. Adding communications beyond, perhaps, voice enhancers (no power required) will not be possible. Because of the weight and size restrictions it is probable that the filter elements will be lighter and smaller than those in PPE.2 (*Long-Term Respiratory Protection – O_2 Available*). Thus the elements must be at least as effective as those required for PPE.2 (*Long-Term Respiratory Protection – O_2 Available*) filter masks, even though the time of use will be much less.

Gap Fillers:

Research and development for escape masks has goals that are so similar to those for ordinary filter masks that the research program for the former ought to derive from the program for the latter. Thus lighter mask materials, more efficient sorbents, better designs for the filter, voice enhancement and so on should arise in the PPE.2 (*Long-Term Respiratory Protection – O_2 Available*) program and simply be adapted for PPE.5 (*Escape Respiratory Protection*).

Personal Protection and Equipment Response Technology Objectives (PPErto)

The roadmap shows the recommended programs with their proposed funding as a function of elapsed time. Even with the overlaps in timing the chart tends to look linear. Yet R&D is seldom linear; rather, it is usually carried out with many starts and stops, recursive loops and so on. Furthermore, the expenditures appear to be steady across each bar when, in fact, there will be ramp-ups and ramp-downs within each bar. Separate RTOs are recommended for each of the five functional capabilities; however, as noted below, extensive coordination among the first three will be necessary. For the first three, the programs begin with exploration of new concepts going beyond what is currently in use or in active R&D already. This exploration is basic research; it should produce new concepts to meet the goals. There follows a period of applied research, beginning while the basic work is still going on. This research is to shape the basic concepts into working constructs that will solve one or more goals. This work will lead to

development of ideas into prototype working models suitable for test, evaluation and demonstration (T&E). Since cost is a significant barrier already for emergency responders and since new technology often comes at a higher cost than that which it replaces, engineering work for both cost reduction and easier producibility is a separate bar.

Finally, there must be integration across most of the functional capabilities. To express this properly would require another dimension. In particular the results of PPErto.1 (*Body Protection – Basic and Applied Research*), PPErto.2 (*Respiratory Protection – O_2 Available*) and PPErto.3 (*Respiratory Protection – O_2 Deficient*) must be compatible with one another. The most effective means of assuring this integration is to have it going on continually from the outset. Some sort of coordinating committee should be set up with representatives from the R&D performers, the manufacturers, and the ultimate users.

For PPErto.1 (*Body Protection – Basic and Applied Research*), the current academic work and basic research in nanotechnology should produce new materials technology for fabrics that will have a degree of "smartness." This work will combine with explorations of other concepts to achieve the one-suit-fits-all goal. Applied research will develop the new designs needed to incorporate the new concepts and will provide the basis for constructing prototypes for development work. Integration is for both backward compatibility with existing suits and masks and for compatibility with new masks in PPErto.2 (*Respiratory Protection – O_2 Available*) and PPErto.3 (*Respiratory Protection – O_2 Deficient*).

For PPErto.2 (*Respiratory Protection – O_2 Available*), the work will focus on lighter weight and more effective removal of toxins for longer time periods. This means materials research for lighter mask polymers and research on new sorbents with higher capacities and effective over a broader range of toxins. There will be studies of various designs for the filter packs, as well as for the mask/filter combination. The mask must be integrated into the suit mask combination of the future.

For PPErto.3 (*Respiratory Protection – O_2 Deficient*), weight and duration of use are the key goals. Materials research on the mask polymers and on the tank should provide some improvement. Finding means of absorbing large quantities of air in a bed of sorbents especially created for air absorption should allow storage of much more air at only moderate pressures. The results must be integrated with PPErto.1 (*Body Protection – Basic and Applied Research*).

For PPErto.4 (*Decontamination*), there are two technical routes to be pursued. One is to find decontaminating solutions that are less harmful to equipment, suits and the like and to the environment. The other is to discover and make into products, self-decontaminating fabrics such that toxins are rendered harmless on contact and less external decontamination is necessary. The latter approach is included in PPErto.1 (*Body Protection – Basic and Applied Research*).

For PPErto.5 (*Escape Respiratory Protection*) the only technical work that should be needed is to adapt the results of PPErto.2 (*Respiratory protection – O_2 Available*). The escape mask is essentially a downgrade of the new filter masks. The biggest challenge here is the size and weight limits. One expects that the higher effectiveness of the new filter agents as well as the lighter weight mask materials – both coming from PPErto.2 (*Respiratory Protection – O_2 Available*) – will enable meeting the weight and size goals.

PPErto.1 – Body Protection – Basic and Applied Research

Objectives:

Devise new concepts for improved body protection and create the basis for prototypes. The ultimate goal is to provide the basis for a one-suit-meets-all-goals system. Research findings from the DoD's large investment in this area will be fed into this activity, as will be results from Strategic Research Areas described in Chapter I. The costs below are in addition to existing programs and fundings.

Payoffs:

The results will provide the basis for prototypes to be used for development and commercialization of an advanced system of body protection that meets all threats with a minimum of specialized add-ons. There will be more protection at an overall reduced cost to the responders.

Challenges:

Obtaining improved performance for all threats at reduced weight will involve trade-offs between sets of mutually opposing requirements. Meeting the one-suit-meets-all goals requirement may be a stretch that cannot be completely met.

Milestones/Metrics:

FY2005: Basic and exploratory research to define the fundamental concepts to be used. Review the best of ongoing work in the federal labs and universities to lay the base for further new concepts. Launch a coordination committee.

FY2006: Continue the basic and exploratory work and begin applied research on the combined goals of the one-suit-fits-all-needs concept. Emphasize microclimate cooling, ballistic and bomb fragment protection, and new fabric constructs.

FY2007: Complete the basic research. Begin integration of findings from all programs and begin work on prototypes.

FY2008: Continue applied research and begin advanced development of the prototypes. Work on manufacturability and cost challenges.

FY2009-2011: Continue development work through FY2011. Final product is a field-demonstrated technology for a one-suit-fits-all-needs protective suit.

The proposed program in this plan is to complement the DoD efforts, not duplicate it. It should begin with basic and exploratory work apart from nanotechnology for three years. Beginning a year and a half into the basic program (see PPE Roadmap) applied research will convert the new concepts into materials and designs suitable for development work. Principal outcomes will be: scientific and engineering reports describing the new concepts and designs along with appropriate patent disclosures. The applied work will produce the basis for prototypes used in the development phase.

This work will explore new fabrics and assemblages of fabric types with the goals of preventing toxins from entering, providing strength and toughness, reducing weight, increasing comfort and dexterity. Some ideas include controlled permeability, microclimate control, fibers from nanotechnology, and reactive substituents to neutralize the toxins.

PPErto.1 – Budget in Millions

Thrust	2005	2006	2007	2008	2009	2010	Totals
Body Protection Research	$2	$9	$10	$18	$10	$15	**$64**

PPErto.2 – Respiratory Protection – Oxygen Available

Objectives:

Discover and demonstrate new materials and filter and mask designs to achieve longer duration (>12 hrs), lighter weight (<10 oz.), effective against all toxins, low breathing resistance (at a peak breathing volume of 400 liters/min), and meets the cost target of less than $300 per unit. The mask should be serviceable at the responders' home station rather than at the factory.

Payoffs:

Present filter masks suffer from the need to change filter packs for different toxins and from high breathing resistance. The new filter mask will provide much longer time in use, be lighter, and have less breathing resistance, be effective against all toxins, as well as meet the cost goal. The responder will be able to wear the mask longer and be much more comfortable in it.

Challenges:

Improving effectiveness and lengthen service life, while at the same time reducing mask weight, will involve some difficult trade-offs. To meet the weight objectives will require new sorbents in the filters that take up much larger quantities of

toxins than heretofore. This means new materials, perhaps from developments in nanotechnology. This will make use of results from Strategic Research Areas in Chapter I (Introduction).

Milestones/Metrics:

FY2005: Basic and exploratory research, searching for a universal filter element effective against all hazards. Study and evaluate candidates from nanotechnology research across the nation.

FY2006: Continue basic work including work on new lens systems with better antifogging properties, communications systems within the mask and begin applied work on most promising candidates.

FY2007: Continue exploratory research and start formulation of one or two prototypes. Conduct integration work of proposed prototypes with results of the other functional capabilities' research.

FY2008: Complete exploratory work on secondary characteristics. Continue applied work on prototypes. Make sure the prototypes can be manufactured at reasonable cost.

FY2009: Continue construction and laboratory testing of prototypes. Begin field demonstrations.

FY2010: Continue work on manufacturability and cost. Carry on field demonstrations, recycle to lab and back to field.

PPErto.2 – Budget in Millions

Thrust	2005	2006	2007	2008	2009	2010	Totals
Respiratory Protection Materials and Designs – O^2 Available	$3	$4.5	$7.5	$10.5	$6	$9	**$40.5**

PPErto.3 – Respiratory Protection – Oxygen Deficient

Objectives:

Discover new air storage concepts and improved materials for self-contained breathing apparatus. Increase in-service time from less than one hour to four hours. Meet weight and cost goals, design ergonomically for function and comfort. Improve seals and face pieces, communications, and indicators of remaining useful life.

Payoffs:

The much longer in-service time (up to twelve hours) will mean that responders can accomplish much more in the hot zone, and trapped or isolated personnel can await rescue more safely. Effectiveness will be aided by the reduced weight (10 oz.) and improved materials, seals, and comfort. The mask will be effective against all hazards and have a shelf- or on-the-belt life of five years. The result should be designed so as to be compatible with the new suit developed in PPErto.1 (*Body Protection – Basic and Applied Research*).

Challenges:

Technology for absorbing large volumes of air at relatively low pressures does not exist. New sorbent materials based on nanotechnology are being discovered now. Decreasing weight while improving performance represents a difficult trade-off.

Milestones/Metrics:

FY2005: Basic research on new sorbents for air to increase life without increasing tank pressure. Look at cage structures, nanotubes and buckeyballs, compare with research findings in hydrogen fuel storage.

FY2006: Continue basic research. Investigate new rebreather concepts. Begin applied work to build new tank storage.

FY2007: Complete basic work and recommend one or two concepts for application research. Begin development work on new concepts. Integrate as many of the goals as possible and integrate with results of the other RTOs in this NTRO. Begin manufacturing and cost control studies.

FY2008: Begin test and evaluation studies on evolving prototypes. Continue building prototypes and evaluating in the laboratory and field.

FY2009: Complete all work. Results are one or two fully demonstrated and field evaluated breathing apparatus suitable for use when oxygen is deficient.

PPErto.3 – Budget in Millions

Thrust	2005	2006	2007	2008	2009	Totals
Respiratory Protection Materials and Designs – O^2 Deficient	$1.5	$3	$4.5	$15	$16	**$40**

PPErto.4 – Decontamination

Objectives:

Discover and demonstrate new ways to neutralize toxins on responders clothing and gear. Explore more environmentally friendly chemical wash systems that are quick – <1 minute exposure – and thorough. Find means of determining the completeness of decontamination. Devise reactive chemical substituents on clothing to neutralize all toxins.

Payoffs:

Current methods do not have the confidence of responders; they are loath to reuse decontaminated clothing. The cost savings from reuse will be considerable.

Challenges:

Developing techniques for determining the completeness of decontamination will be difficult. Removing the present psychological block to reusing the decontaminated clothing will require study into the phenomenon and education combined with reliable new technology.

Milestones/Metrics:

FY2005: Applied research on new systems proposed elsewhere. Consider new chemical concepts and compare and contrast with the current chlorine-based approaches. Review results of work on self-decontaminating fabrics work being done in the DoD as well as elsewhere.

FY2006: Continue studying proposals from earlier work. Select one or two systems for prototype development.

FY2007: Develop prototypes and evaluate in the laboratory. Begin test and evaluation in field demonstrations.

FY2008: Complete field demonstrations. Carry out manufacturing and cost studies.

FY2009: Complete manufacturing and cost studies.

PPErto.4 – Budget in Millions

Thrust	2005	2006	2007	2008	2009	Totals
Decontamination Technologies	$2	$3	$4	$7	$6	**$22**

PPErto.5 – Escape Respiratory Protection

Objectives:

Develop an improved version of escape hood: more compact, lighter, with a shelf-life of five years, and effective against all hazards and at a unit cost of about $100.

Payoffs:

The hood will fit on the responder's belt and will be especially useful for law enforcement officers first on-scene.

Challenges:

To be at once smaller, lighter, and more effective presents a severe difficulty and must entail a new much more effective filter element and lighter mask materials.

Milestones/Metrics:

(Since the technology will be the same as for the new filter masks (PPErto.2 (*Respiratory Protection – O_2 Available*), the same basic and applied research will be needed. Using the results of PPErto.2, only development work and adapting the results will be required. The development work will begin after the fourth year of PPErto.2 and run for three years.)

FY2005: None

FY2006: None

FY2007: None

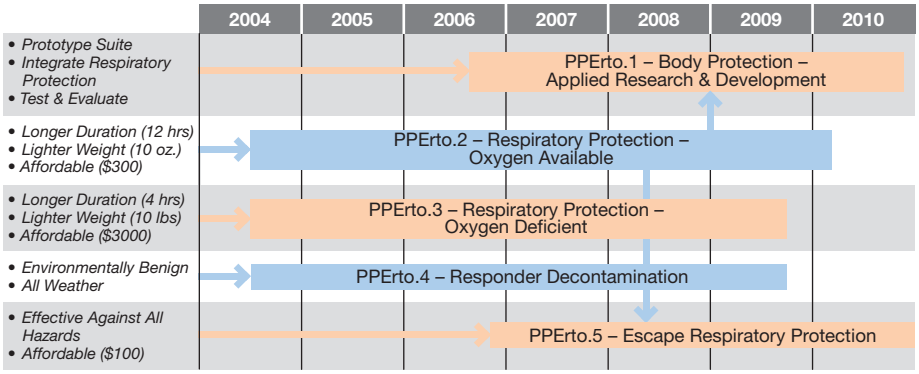
FY2008: Adapt technology from PPErto.2 (*Respiratory Protection – O_2 Available*) to escape masks. Build prototypes. Begin development work on prototypes.

FY2009: Continue development work. Conduct demonstrations.

FY2010: Complete development work with field experiments.

PPErto.5 – Budget in Millions

Thrust	2005	2006	2007	2008	2009	2010	Totals
Escape Respiratory Protection	$0	$0	$0	$0	$2	$4	**$6**



Personal Protection and Equipment Technology Roadmap

Chapter III

Detection, Identification, and Assessment (DIDA)

Chapter Chair: Dr. Jasper Lupo
Chapter Coordinator: Michelle Royal

Definition

Detection, Identification, and Assessment (DIDA) is the capability to quickly detect, locate, characterize and assess a potential or ongoing terrorist attack. DIDA consists of sensor and related information technologies and capabilities that can provide responders with knowledge to deal as effectively as possible with terrorist events involving weapons of mass destruction.

Operational Environments

In considering DIDA, responders focused on pre- and post-attack capabilities against five categories of terrorist attack: *chemical, biological, radiological, nuclear, and explosive/incendiary*. In practice, they divided these five into two groups. The first group, consisting of the chemical, biological, and radiological (CBR) attacks, requires some means of dispersal in air, food, water, or other media and causes injury or death through inhalation, ingestion, or bodily contact. By contrast, nuclear, explosive, and incendiary devices (NE) have their primary effects through blast, pressure, and fire. Responders are also concerned that more than one type of device might be used in an attack.

DIDA can be hindered by terrorist use of decoys, deceptive techniques, secondary devices, and countermeasures that shield, hide, saturate sensors, hinder discrimination, or disguise the weapon. These countermeasures are obviously relevant prior to release or detonation. However, the use of post-release countermeasures must be considered in order to avoid surprise from more sophisticated compound attacks that could come in the future.

In DIDA, responders considered all stages and levels of the threat spectrum, but with primary emphasis on response:

- *Prevention* – pre-release, pre-event defensive measures to prevent, reduce vulnerability, and minimize consequences prior to terrorist use of the weapon. The *prevention* stage may span minutes to years. Upon warning of an impending event, responders will attempt to detect, locate, identify, assess potential damage, isolate, and disarm a weapon of mass destruction. This NTRO deals with the detection through assessment portions of the operation. Note that many of the sensors used to accomplish this are also useful in the long periods of vigilance leading up to the tip-off or emergence of an impending threat.

- *Response* – capabilities needed following release or detonation, during the period in which people are in danger. *Response* may last from minutes to days, depending on the severity of the attack and the nature of the weapon. Here DIDA may provide the initial detection that an attack has occurred. It would also be used to rapidly provide on-site information about the weapon, the victims, and the extent of damage. This information is needed so that responders may also protect themselves if possible as they proceed to help the victims and avert further damage. The response phase also includes the prevention of further damage from secondary devices by detecting their presence and facilitating their deactivation.

- *Consequence management* – post-event sensor and information capabilities that facilitate recovery, aid cleanup, and improve treatment of victims. At some point in time, response will become *consequence management*, restoration and recovery. This may happen over hours to days, weeks, or much longer if the event is severe. In recovery, DIDA provides critical information needed to prevent further infection or exposure to residual agents, aid in cleanup, define quarantine and keepout zones, assess structural integrity, and determine habitability of buildings.

Responders and technologists discussed differences among the five attack modes and what they mean to DIDA; their findings are summarized below.

Chemical Agents – Chemical weapons can be broken up into three classes: toxic industrial chemicals such as phosgene, injurious chemical warfare blister agents such as mustard gas, and lethal chemical warfare agents such as nerve gas. Dispersal is a key parameter in the use of chemical weapons. Detection and identification of dispersed chemical agents has received a lot of attention for both industrial and anti-terrorist purposes. Sensor technology tends to be relatively mature, although there is an issue with false alarm rates if there are similar, confusing chemicals (interferents) in the environment. Volatility and persistence of various chemical agents can also dramatically affect detection strategy. Inexpensive, rapid field sensors that can handle a spectrum of agents are in development. Stand-off and remote detection of chemical agents in containers is very difficult, but progress has been made with sensing schemes that involve contact or very close proximity with the reservoir. The DoD R&D activities are making good progress in the detection of chemical aerosol plumes.

Biological Agents – the Poor Man's Nuke. Biological weapons and agents are quite diverse: DIDA must handle a wide range of threat agents, including bacteria, viruses, spores, and bio-toxins, both those occurring in nature and those that might be altered or engineered in the laboratory. Bio-toxins are not living organisms and behave more like chemical agents. Some bioagents are contagious, complicating containment and tracking of the attack. Some are intended to disable and others to kill. The lethal doses vary dramatically by agent type and the age and health of the victim. As with chemical agents, bioagents are nearly impossible to detect until they are used. They are even more easily concealed than chemical weapons because extremely small containers may contain enough agent to affect tens of thousands of people – biological agents can be 100 to 1000 times more lethal than chemical agents. DIDA of released bioagents is also relatively mature in the laboratory and in controlled environments. However, rapid, affordable detection and identification in the field is more difficult than in the case of chemicals due to the fact that lethal agents may be virtually indistinguishable from harmless counterparts.

There is generally more time to deal with the effects of a BW attack than with chemical and bomb threats. The exposed population may not begin to exhibit symptoms for seventy two hours or more. This typical delay produces a danger and also an opportunity. The danger, especially in the case of contagious agents, is that the delay will impede the identification of carriers of infection who have dispersed from the attack site before the existence of an attack has been recognized. The opportunity is that detection of an attack can provide an opportunity for containment and treatment efforts that may prevent onset of the disease or reduce its effects.[6]

Radiological Agents – A so-called dirty bomb is made of radioactive materials dispersed by conventional explosives. A small quantity can contaminate a large area and affect a large number of people. These agents are not well suited to producing large numbers of fatalities but they can cause panic, long-term illness, and deny use of

[6] Many bacterial diseases can be treated effectively with antibiotics if the exposure and nature of the agent is recognized in time. Even where no effective specific treatment is available (as in the case of most viruses today), non-specific medical care and preventing secondary infections can contribute importantly to survival.

key facilities or neighborhoods. Depending on the isotopes used, danger may persist from hours to centuries. Unlike CB agents, radiological substances can be detected before release because radioactive materials emit gamma rays and neutrons that can be detected at useful stand-off ranges (tens of meters for unshielded devices). Sensor technology is relatively mature and compact. Portable radiation detectors in pager and cell-phone-sized packages are commercially available and used by some responders. However, no handheld, compact device is now available that can identify isotopes in the field. Field ID is possible in fixed, vehicle, and man-portable hardware that tends to be too expensive for widespread use. Although DIDA at modest ranges is possible, shielding can dramatically reduce the effectiveness of sensors and their range. On the other hand, shielding is heavy and makes concealment more difficult than with chemical and biological agents. Cleanup is conceptually easy because the agents radiate, thus facilitating delimitation of contaminated areas and equipment.

Nuclear Weapons – Because of the enormous power of nuclear weapons, and the devastating nature of their effects, time is the critical factor in the prevention phase of an event. Prior to detonation, it is possible to tell the difference between legal radioactive materials, a dirty bomb, and a nuclear bomb. Unshielded weapons can be detected at tens of meters. Nuclear weapons are large and heavy when compared to CBR agents; they are much harder to carry and conceal. If extra shielding is used to conceal the weapon, the added weight makes it even more difficult to transport these weapons, and the shielding itself may be subject to detection. Although an individual can carry a technologically advanced low-yield weapon, vehicles are the more desirable means of moving them around. If nuclear detonation is achieved, simple detection is no longer an issue. Assessment for nuclear weapons combines all the capabilities for radiological plus explosives and incendiary devices, and identification/attribution would use very specialized capabilities possessed by the Department of Energy and its National Laboratories.

Explosive and Incendiary Devices – Bombs like the Oklahoma City and Khobar Towers devices are large, vehicle-transported weapons. Stand-off detection of the explosives in bombs and incendiaries is difficult, but progress has been made and responders consider this a manageable DIDA problem. Detection usually relies on stand-off and proximity sniffing for nitrogen compounds. Suicide bomb vests may be detectable through clothing with imaging or acoustic systems that do not detect the explosive material itself, but rather a visual shape or indication of unusual density that may help intercept the carrier.

Needed Functional Capabilities and Priorities

Responders and technologists considered a set of Functional Capabilities to handle the operational context described above. The capabilities are presented below in order of priority, the first being the highest. They are grouped into four categories reflecting break-points between the degree of priority as judged by responders. These rankings were provided in workshops and interviews.

- On-Scene Detection

- Remote and Stand-off Detection
- Classification and Mitigation
- Non-Intrusive Stand-off Inspection
- Detector Arrays and Networks

- CBRNE Effects Modeling and Simulation
- Collection and Dissemination of Weather and Environmental Conditions
- Pre-Triage/Differentiation Among Levels of Exposure

- Rapid Assessment of Structural Integrity/Other Risks
- Remote Detection of Deception

Overall State of Technology for Detection, Identification, and Assessment

The matrix on the next page shows a mix of moderate to high technological challenges in raising the level of capabilities for emergency response. The section that follows lays out a number of Response Technology Objectives that will address key areas for high-payoff technology development.

Detection, Identification and Assessment

Functional Capabilities	Operational Environments: Chemical	Biological	Radiological	Nuclear	High Explosive/ Incendiary
1. On-Scene Detection					
2. Remote and Stand-off Detection					
3. Classification and Mitigation					
4. Non-Intrusive, Stand-off Inspection					
5. Detector Arrays and Networks					
6. CBRNE Effects Modeling and Simulation					
7. Collection and Dissemination of Weather and Environmental Conditions					
8. Pre-Triage/Differentiation Among Levels of Exposure					
9. Rapid Assessment of Structural Integrity/Other Risks					
10. Remote Detection of Deception/Intent					

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

Detection, Identification and Assessment

DIDA.1 – On-Scene Detection. *The ability to detect danger to self (responder) and others.* This capability, ranked as the highest priority by responders, focuses especially on initial detection before an attack, or, after agent release but before the onset of symptoms. It includes: characterization of suspicious objects; detection in the presence of decoys and countermeasures; detection of secondary devices; and the post-attack location of the source of an agent release or a device that may be continuing to release the agent. Wearable, man-portable, and vehicle-mounted devices are needed.

Distinction was made between systems that are expensive or that require highly trained users and inexpensive and easy-to-use systems. The former are likely to be used by a few specialized response units that are unlikely to be first on the scene and that therefore are unlikely to contribute to initial detection; the latter could be proliferated throughout public safety forces and thus might provide a real possibility of affording initial detection. Even among capabilities that can be widely proliferated, there is an important distinction between wearable sensors that are carried at all times by police officers and firefighters, and bread-box sized or larger units that would normally remain in a vehicle.

Great emphasis was given to wearable sensors. The workshop also noted that it would be burdensome or unacceptable to require emergency responders to carry multiple sensors to span the sensing needs for full spectrum CBRNE on-scene detection, even if each were the size of a cell phone. It was suggested that an integrated device is needed. This is the subject of a suggested development program.

Goals:

- Accurate, rapid, reliable, affordable.
- Minimum logistics tail (power requirements and consumables).
- Wearable, man-portable, and vehicle-mounted devices.
- Ability to detect presence of decoys, counter-measures and secondary devices.
- Ability to locate source, vessel or vector.
- Communication link to command center – potentially allowing alerting and subclinical information to be integrated without operator intervention.
- Adaptable for use on robotic platforms for penetration into hot zones too dangerous for immediate entry by unprotected responders.

Current Capabilities:

Responders are aware of the wide variety of sensors on the market and pointed out in the workshop that they do not have or use them because they are too expensive and difficult to use.

- Emergency responders rely almost completely on information from calls received at the dispatch center, with no initial on-scene information.
- Patrol officers have no sensors at all.
- Chemical detectors exist but are too large (useful for specialized units only).
- Radiological dosimeter pagers are not widely deployed.
- There is no capability available to local responders for pre-release nuclear detection, although federal responders may have the capability.
- Biological sensor capability is very limited or unavailable; known commercially available equipment is costly and somewhat delicate, making it suitable only for personnel with specialized skills and training.

State of the Art:

Technologists noted that much has and is being done to support the goals for on-scene detection. They noted that nearly all existing systems are the result of past and current military R&D. See the chart below for a detailed survey of CB detection programs from the April 2003 *Integrated Chemical and Biological Defense Research,*

Technology Group	Programs		Shared Technology Platform
Detection and Identification			
Genetic Detection	• HANAA	B	PCR for genetic detection of bacterial and viral agents
	• Auto Genetic ID	B	
	• APDS	B	
	• PCR DTB	B	
	• Field Sample Extractor	B	
Detector on a Chip	• Argonne MAGIChip	B	Microchip platform for detection
	• Advanced Multi-function Biochip	B	
	• Gene Chip Biosensor	B	
	• Activity Based Detection and Diagnostics	B	
Mass Spectrometry	• BSPS-ESI/MS	B	Mass spectroscopy methodologies for sample handling/analysis
	• SESI IR MS	B	
	• Bio-ToF MS	B	
	• Advance Ion Trap MS	B	
	• Real-Time Bio MS	B	
Handheld Systems	• CADB	C	Systems optimized for handheld use
	• µChemLab/CW	C	
	• µChemLab/BW	B	
	• µChemLab/CB	CB	
	• Personal Alarm Monitor-BW	B	
	• Personal Alarm Monitor-CW	C	
	• UCPHHA	B	
	• SMALLCAD	C	
	• Handheld Low-level CAD	C	
	• Maritime TICD	C	
Other	• Immunobead Force Differentiation Assay	B	N/A – Each platform is unique
	• Amplifying Fluorescent Polymer	CB	
	• Pyrolysis-GC/Ion Mobility Spectrometry	B	
	• Optical Particle Classifier	B	
	• CB ID in Water	CB	
	• Integrated CB Point	CB	
	• DCASTS	C	
Reagent/Assay Development			
	• Biocontaminant Detect/ID Strategies	B	Goal of programs is shared, but the nucleic acid-based program differs from the antibody programs
	• Nucleic Acid-based Assays	B	
	• Reagent Development (antibodies and alternatives)	B	
	• Immunoassays	B	
	• Protein Signatures	B	
Supporting Technologies			
	• Ambient Background Characterization	B	Immature technologies not yet fully defined; will eventually contribute to the bio point detection technologies listed above
	• Aerosol Sampler Development	B	
	• Threat Agent Characterization	B	

Ongoing CB Detection Programs as of 2003

Development and Acquisition Plan: Chem-Bio Point Detection (p.11). This plan outlines the major efforts by the DoD, DoE, and TSWG.

Chemical – A number of chemical detection devices and technologies are emerging and should become available for commercial transition; JCAD, Gas Chromatography Surface Acoustic Wave (GCSAW), IMS, traffic light sensor, SMO (metal oxides), enzyme based devices, tissue based sensors, activity based sensors, cell based sensors, Raman spectroscopy, dual GC, aerosol gel (C&B), Smart Card, miniature Flame Ionization Detector (FID), Flame Photometric Detector (FPD), LPOSS, Polychromator chip, Iontrack, mass spectrometry; and combinations such as SAW/IMS.

Biological – Immunoassay (manual, automated), genetic assay (manual, automated polymerase chain reaction (PCR)), particle detection/classification, multiple optical approaches, capillary electrophoresis, pyrolysis/ion mobility spectrometry, cell-based sensors, mass spectrometry, laser induced breakdown spectroscopy (LIBS), automated sample collection and preparation, host expression of genetic markers, synthetic ligands, and bio-detectors on a chip, such as Canary – a Lincoln Laboratory development which may soon be ready for application.

Radiation – As mentioned earlier, there are commercially available handheld gamma ray detectors. However, there is no discrimination capability, and the devices do not detect neutrons. A handheld, combined gamma ray and neutron detector with built-in discrimination capability is needed to reduce false alarms associated with normally occurring medical and industrial sources. Work toward this end is underway at Department of Energy (DoE) laboratories. While alpha and beta radiation may be less of a threat to produce mass casualties (particles must be inhaled or ingested or enter the skin through wounds to be dangerous, and thus efficient dispersal and control of particle size would be necessary), responders need detectors sensitive to emitters of this sort of radiation, as well to be prepared against all hazards and to ensure full decontamination of radiation sources.[7]

A major gap was noted: responders need an integrated wearable CBRNE sensor suite that is easy to use, nearly automatic, and requires little or no training to use properly. It was noted that almost all sensor work is concentrated into specific sensor stove pipes such as chemical or biological. Each community has its own expertise and technical issues that consume resources and challenge the limits of detection science. Thus there has been little motivation or funding available to pursue integrated devices. See the chart on page 35 (Ongoing CB Detection Programs as of 2003).

Technology Limitations and Barriers:

The most prominent limitations are the false negatives and positives associated with the detectors for all threats. Most reliable CB detectors require contact with the agent, and in fact, collect and intensify the agent to get enough to be detectable. This is complicated by the fact that the environment has substances that may be confused with threats or add to the noise of the sensor. There is a need to characterize, and then rapidly and accurately adjust to fluctuations in the background produced by these ambient substances. Certain biodetection technologies are agent specific; there is the possibility that new agents may be rapidly engineered that do not exist in any library or detection inventory. On the other hand, more general detection strategies may fail to provide a clear picture of the agent and what to do about it. It is likely that a layered approach will be needed, and that the handheld devices will only be able to provide capability against a limited set of known agents.

Handheld and wearable chemical and nuclear detectors exist in separate packages. Algorithms for the discrimination of radioactive isotopes using sodium iodide detectors also exist but handheld devices do not currently offer

[7] Fortunately, most alpha and beta emitters also emit detectable levels of gamma radiation; otherwise they would be hard to detect at a distance through the air unless present in very large quantities. Detectors and procedures are available that, at least in skilled hands, allow the rapid characterization of all radiological hazards and assessment of the degree of decontamination. Packaging these capabilities for use by personnel with less-specialized training is still something of a challenge.

discrimination capability. Bioagent detection technology for wearable sensors is not as mature. PCR technology cannot be packaged to fit in a handheld device. Immunoassay systems might provide capability for a small number of bioagents, although sensitivity would be limited to high-level attacks. Emerging biochips offer the best hope for combined sensitivity, speed, cost and multi-agent handling. Technologists assert that biochips are now ready for commercial application. Hence, the goals of DIDA.1 pose a major engineering and packaging challenge to combine all in one wearable unit, but no fundamental science issues.

Current biological detectors are slow and take anywhere from twelve minutes to one hour to produce reliable results in the field; other limitations include poor portability, the need for costly reagents that must be replenished whether used or not, sample collection and preparation, and cost of reagents and processing fluids. It was noted that genetic engineering of agents poses a limitation on our ability to recognize new bioagents; it is currently easier to quickly design a new agent than to figure out how to detect it in the environment, and commercialize the reagents and processing needed for on-scene detection. There is also growing but limited knowledge of virulence factors that may be useful for characterization and assessment of organisms.

The vast majority of responders do not have on-scene radiation detection and discrimination capability; although the underlying technology is considered mature by many technologists. Radiation pagers and dosimeters do exist but they cannot generally distinguish between isotopes in the body from medical procedures and terrorist threats. On-scene radiation discrimination for the responder simply does not exist.

It was noted that little is being done to combine sensor types into multi-sensor packages. Ease of training and ease of use were cited as deficiencies with current sensors; there is a need for devices that require little, easy or no training. Electromagnetic interference was cited as a factor that could degrade sensor processor performance. In the case of a nuclear attack, the electromagnetic pulse could damage sensitive electronic components outside the blast zone.

Finally, with regards to wearable sensors, the ability to package a full CBRNE detection and discrimination suite in something the size of a personal digital assistant (PDA) will require significant R&D. Currently, the weights and sizes of individual handheld devices (with their known limitations) for each threat are all somewhat larger than a single PDA.

Gap Fillers:

An integrated handheld, PDA sized, CBRNE sensor would fill the major gap noted during responder discussions. Combination of existing and emerging sensors in one handheld device will be a significant challenge. Ease of use and training will be a necessity since this device would probably be issued at the scene to responders who have had little or no prior opportunity to use it. If possible, the detectors should rely on techniques that do not use expensive or perishable consumables and reagents. The device will need to be rugged, environmentally hardened, and easily decontaminated. Even if such a device can be made, an important issue will be the concept of operations for its use. For example, will the wearer get an immediate alarm or will data be collected for use by leadership? Some experts express concern about public panic or hysteria, but this may be less of an issue for devices designed for use by responders rather than an untrained populace. See the associated technology objective, DIDArto.1, *(Wearable Integrated CBR Sensors)*, and the DIDA roadmap for details.

DIDA.2 – Remote and Stand-off Detection.

The ability to identify and assess the severity of an attack, and define keep-out areas from outside the hot zone, remotely examine clouds for agents and other harmful particles, and assess the levels of radiation in an area. Stand-off ranges of up to one kilometer are desired. This may be accomplished through the use of true remote sensors and/or point sensors on mobile robotic ground and air vehicles; currently even trained dogs and other animals are used to carry sensors. Sensors that actually enter the hot zone are in fact point or

embedded sensors and rely on close-in detection methods or exposure to the agent; the sensing mechanisms for these are covered in other capabilities. See DIDA.1 (*On-Scene Detection*), DIDA.5 *(Detector Arrays & Networks)*, and DIDA.7 *(Collection and Dissemination of Weather and Environmental Conditions)* for discussion of such detector technologies.

Goals:

- Responders want aerosol plume, cloud assessment and identification from stand-off ranges of up to one kilometer.
- Detection of harmful CB agents and radiation levels with low false alarm rates.
- Compact, easily operated, automatic systems are needed for use by responders who deploy to a scene in a vehicle.

Current Capabilities:

- No remote chemical detection is used by responders even though the military has had items in the field for over ten years; the National Guard Civil Support Team has a vehicle mounted threat sensor. There are no convenient man-portable sensors.
- Radiological remote sensors such as gamma ray imaging systems for nuclear plants and associated accidents exist. However, they work at ranges of a few meters and are slow, even against very high levels of radiation encountered in spills of nuclear waste or meltdown situations.
- Biological plumes: no current operational capability for remote sensing exists for civilian use. Military devices are developmental. Some concepts rely on penetration of the plume with robots to collect samples for later analysis. Chem/bio plume tracking is currently a priority in military R&D.
- Explosives sniffing robots are useful but too expensive for wide proliferation, although they do provide a means for getting sensors into areas that may be too dangerous for the responder. Dogs are often used by civilian responders to detect explosives. Several breeds are used, depending on the task and preference of the user. Sense of smell varies from 100 to 1000 times better than human beings. Hound dogs and beagles are the most sensitive, whereas collies and German shepherds are smarter. Attention span is an issue; smarter dogs tend to get bored more quickly. Dogs can be trained to detect a wide variety of substances. One drawback with dogs is that they require care and feeding whereas robots can be stored until needed.

State of the Art:

Remote and stand-off detection of chemical clouds has been in the military inventory since 1990 and was deployed in the 1991 Gulf War. However, these military units are not designed for civilian use. Civilian needs for wide area surveillance could best be met by a network of permanent sensors that measure spectral transmission over modest path lengths.

There are a number of existing programs with applicable technology for chemical sensors. Fourier Transform Infrared spectroscopy (FTIR) is deployed in military fielded instruments; it is expensive, detects nerve agents and toxic industrial chemicals (TICs) but is not very useful against mustard gas. FTIR is passive and can see up to 5 km in ideal conditions. Active laser technology is in military R&D; it holds promise to make maps of cloud density but issues of eye safety as well as effectiveness need to be addressed. There are various concepts for using coated fiber optics either in passive or active stand-off sensors or in robots that penetrate the cloud. Hyperspectral imaging in various spectral regions can detect absorption lines of certain chemical agents and is being considered for Chem/Bio and other aerosol detection jobs as well as civilian environmental monitoring. There is significant industrial interest in this technology. In certain bands, its sensitivity is limited to daylight only; shadows in urban canyons may reduce effectiveness.

For sensing biological agents, ultraviolet (UV) sensing is currently limited by the availability of

powerful, UV laser diodes at wavelengths of interest. This technology may provide useful discrimination out to a few hundred meters. Laser diode technology is under development at DARPA. Currently there are no credible approaches for mid- and near-infrared (IR) detection. DoD is investigating medium wave infrared (3-5 microns) LIDAR systems capable of remote bioagent cloud detection at up to a kilometer. Commercial systems exist (*e.g.*, for remote sensing of gas pipeline leaks), but further research is needed to assess their potential for stand-off detection of bioagent clouds.

For sensing radiation and high explosives/incendiary weapons, Sandia National Laboratory's Second Line of Defense (SLD) Program has been deployed in the Former Soviet Union, to prevent the smuggling of nuclear devices and material through key choke points. DTRA has installed a variety of radiation and bomb detection testbeds at four military bases in the U.S. as part of the Unconventional Nuclear Weapons Defense Program. The sensors used on these bases are too large and expensive for easy use by responders. There are very large systems that can image through container walls to give the responder a picture of the contents, including people. One system uses x-ray scanning in a large van and the other uses gamma rays. These systems are very costly and best used at loading areas and weighing stations. Millimeter wave imaging has been developed for short-range imaging through non-metallic walls. Researchers at Los Alamos National Laboratory have demonstrated the feasibility of using naturally occurring muons in cosmic rays for detecting high-atomic weight materials (fissionable material or shielding) for vehicle inspection, but dwell times on the order of one minute are needed.

Technology Limitations and Barriers:

The availability of high-energy UV laser diodes currently limits the range of biological plume detection. The optical transmission of UV is inherently limited to a few hundred meters in the atmosphere, depending on wavelength. Wavelength agile and higher power lasers are needed in general for improved stand-off ranges in CB detection. Sensitivity is poor and limited to dense clouds containing 1800 agent-bearing particles per liter of air. This equates to very dense clouds and does not allow accurate mapping of the lethal boundaries of the plume. Detection of biological clouds from a distance is a topic of military R&D.

True remote radiological and nuclear sensors exist, but are too large, heavy, and expensive for nearly all emergency responders. Range is a few meters, dependent on shielding and whether or not the object is moving. This limit is fundamental and based on background radiation and detector sensitivity. It is very unlikely that any amount of funding will improve the range of these sensors. Physics does not support detection of radioactive isotopes at ranges greater than a few tens of meters, or a hundred meters in ideal conditions. Thus detection of the cloud from a dirty bomb or the fallout from a nuclear weapon would depend primarily on detection of the obscuration using optical, lasers, and or thermal imaging. It would not be possible to identify the cloud as radioactive without prior information or penetrating sensors.

Gap Fillers:

A gap was identified highlighting the need for smaller, proliferable, network oriented radiation sensors with built-in discrimination capability. See DIDArto.2 (*Stand-off Radiation ID*), and the DIDA roadmap.

Suitcase size detection suites would provide detection ranges of a few hundred meters, depending on the agent. Responders noted the need for a relatively compact, affordable solution to on-scene cloud mapping that would combine both chemical and biological detection in one easy to deploy and use package. Technologists suggested that easing up on tough military, combat-driven specifications such as rapid alert time, extended ranges, and detect-on-the-move capability could enable such a development for urban use this decade. Static installation of bi-static designs could improve sensitivity and allow continuous sampling; *e.g.*, transmitter on one building and receiver on another. See DIDArto.3

(*Integrated Remote Detection of CB Agents*) and the DIDA roadmap.

DIDA.3 – Classification and Mitigation. *The ability to integrate sensor data with symptoms and pathology and provide mitigation guidelines for dealing with contamination and injury.* Focus is on the local information tools available to the responder and the ability to correlate observations with a particular event. Responders need a simple tool that walks them through a decision tree and leads to recommended action. It is related to DIDA.8 *(Pre-Triage/Differentiation Among Levels of Exposure)*, which focuses more on the sensing of subtle physiological phenomena associated with pre-triage conditions that cannot be discerned by a busy responder who must deal with the obvious cases.

Goals:

- Comprehensive: All hazards should be covered.
- Immediately available – the responder should not have to wait for input.
- User-friendly, expert system.
- Small, compact PDA size.

Current Capability:

- Responders indicated that they have a wide choice of emerging tools that they could purchase.
- Components exist for each threat of some combinations, but a full threat spectrum needs to be integrated into a system that is immediately available to responders.

State of the Art:

There are many programs that are addressing certain threats. A modest effort is needed to integrate them.

The Automated Decision Aid System for Hazardous Incidents (ADASHI™) is an Army-sponsored, portable, computer-based integrated decision-aid support system for improving the response to a hazardous incident by military and civil responders. ADASHI™ can be used at the site by the Incident Commander (IC) or at operation centers. The tool supports individual and collective training at a responder's home. ADASHI™ is designed to function on laptops and desktop computers.

A number of chemical risk assessment tools and related environmental tools are in development. These decision aids will allow the user to assess the transport of toxic chemicals. They are designed primarily for use by engineers.

Lightweight Epidemiology and Advanced Detection, Emergency Response System (LEADERS) is a medical surveillance tool providing real-time analysis of medical data to identify the presence of a covert or naturally occurring bio-event. Clinical data is collected using specific medical applications and laboratory identification tools.

Sandia National Laboratory developed probabilistic risk assessment (PRA) as a tool for evaluating the risks associated with high-consequence systems such as nuclear weapons and nuclear power generation plants. This tool is used for risk assessments for critical infrastructures such as dams, water utilities, chemical plants, and power plants and might be adapted for responder use (especially for planning before an incident).

The Chemical Biological Response Aide (CoBRA) software contains pre-loaded accredited operating procedures and on-scene checklists designed to address chemical identification, evidence collection, decontamination and general response to terrorist use of a weapon of mass destruction.

The Defense Advanced Research Projects Agency (DARPA) has developed a set of tools, including The Global Response Incident Planner (GRIP) and the Field Inventory Survey Tool (FIST). The program has also created the Playbook Manager. DARPA also developed a program to address the weaknesses in current crisis management systems—the Enhanced Consequence Management Planning and Support System

(ENCOMPASS). This product is an integrated suite of software tools that uses Web-based and standalone software to collect and distribute dynamic data to and from multiple sources in near real-time. ENCOMPASS has two primary subsystems: the Incident Command Management System (ICMS) and the DARPA Syndromic Surveillance System (D-S3). ICMS centers on the functions of the Incident Commander at various levels, including the emergency responder, scene commander, operations center, and/or state/national emergency center. The D-S3 is a biosurveillance capability that tracks patients' signs and symptoms to alert epidemiologists of any new trends, such as the possible release of a biological agent.

Technology Limitations and Barriers:

There are neither technology barriers to meeting the performance goals nor to meeting cost and size goals. A host of products and programs exist, and there are even federally funded efforts in place to help sort through them. This is primarily an information and software integration task. The biggest challenges involve a friendly user interface for the responder and orderly treatment of all the databases and information needed to link knowledge to action.

Gap Fillers:

Responders would like to see the integration of military and civilian programs and processes. Technologists, although appreciative of the need, felt that the maturity level of this capability and ongoing programs is too high to warrant creation of a gap filler technology effort within DIDA. However, it is recommended that the government consolidate its own programs, take steps to maintain a current catalog of available tools, and ensure that responders have adequate information on the value of these tools either through an official or semi-official standards/testing process or through a voluntary responder evaluation process similar to that found on some commercial internet sites. This functional capability overlaps with the requirements for R&Rrto.1.

DIDA.4 – Non-Intrusive, Stand-off Inspection.

The ability to detect pre-release CBRNE materials in packages, vehicles, and on people, without requiring packages or vehicles to be opened. For use at portals for special events, limited areas, containers and at traffic stops. More broadly, the inspection of packages includes mail in the postal system, shipping containers, crates, luggage, cargo in ships and trains, aircraft, and trucks, so there will be overlaps between responder needs and those of various federal agencies and the postal service. Stand-off may be from one meter to a few meters. Although this kind of inspection is generally accomplished using controlled geometry, a relaxation of this constraint would be useful and permit wider use of the equipment. The detection of shielding for nuclear devices is needed for dealing with radiological countermeasures.

Goals:

- Useful ranges from one meter to several meters.
- Accurate, portable, rapid, reliable, affordable.
- Minimum logistics tail (power requirements and consumables).
- Man-portable, and vehicle-mounted devices (less pressing).
- Ability to detect presence of decoys, countermeasures and secondary devices.
- Rapid detection on the order of a few minutes at most depending on range and agent being detected.
- Nuclear/Radiological: Detect unshielded devices and shielding for further inspection.

Current Capability:

- Special event teams have portal magnetometers, imagers, and explosive residue sniffers.
- Responders have no stand-off inspection capability for biological agents and would like an integrated CB capability.

- Radiation pagers exist but are not generally deployed. See DIDA.1 *(On-Scene Detection)*.

- Crowd surveillance/traffic stop systems (unconstrained geomentry) not available.

State of the Art:

Remote detection and identification of radioactive materials is a solved problem for ranges that do not exceed physical limits. Shielding can reduce those ranges but with great weight penalty to the terrorist. At present, non-intrusive detection of chemicals in vessels requires physical contact with the vessel: this includes current applications of ultrasonic technology to detect liquid in containers. Noncontact detection of chemical agents in vessels is a focus of military R&D. There are no known techniques that can provide reliable detection of biological agents in vessels.

The Technical Support Working Group (TSWG) has supported a variety of programs in stand-off explosives detection. They have created a Defense Technology Objective to detect 100 pounds of explosives at ten feet. This program goes to FY2005. UV and X-ray fluorescence programs may also offer solutions to detect, on surfaces, secondary or tell-tale substances associated with threat agents. Other technologies in existence with application to stand-off detection of explosives include acoustic (including dielectric and thermal), prompt gamma ray neutron activation analysis (which does not require contact with container), and laser trace explosives detection.

Technology Limitations and Barriers:

- Currently there is no non-contact method for inspection of CB containers in unconstrained scenarios; there are very few concepts that have a credible theoretical basis for solving the problem.

- Responders consider the affordability of limited available products to be a significant barrier.

- There are no responder tools for detecting dangerous solids within well-sealed containers.

Gap Fillers:

Technologists and responders identified the need for a program for close-in, non-contact, nondestructive stand-off inspection of containers that might contain CB agents. Technologists think that this is a very difficult capability to achieve and that the barriers are formidable. See DIDArto.4 (*Portable Stand-off Container Inspection*), the DIDA roadmap, and the list of issues discussed below.

- Acoustic programs should be extended to non-contact scenarios.

- Radiation detectors should be made more practical: reduced size and cost are needed. See DIDA.1 (*On-Scene Detection*) and DIDA.2 (*Remote and Stand-off Detection*).

- Acoustic detection technology should be explored for detection and identification of solids in containers.

DIDA.5 – Detector Arrays and Networks.

Sensor arrays that can be networked to provide alerts, identification, localization of CBRNE threats; linked to command data centers; to provide environmental monitoring in urban centers, building interiors and sensitive areas. Although ranked fifth in part because they do not fit into existing responder concepts of operations, probably one the most important developments will be sensor arrays that can be networked to provide alerts, identification, and localization of CBRNE threats. There is a growing need for compact, low-cost, minimal care, automatic detectors to enable the fielding of widely distributed, heterogeneous sensor arrays and networks. These sensor webs should be tied to command data centers through wireless and/or wired communications links. Data derived from the arrays will localize source and project danger areas using physical models and 3-D GIS. They will provide environmental monitoring in urban centers, building interiors, and mobile nodes with the capability for automatic alarms. Distributed data collection will enable event tracking and characterization. Sensors should adhere to standard outputs and input commands through commercial interfaces

such as Universal Serial Bus (USB) to ensure interoperability and rapid insertion into the network.

Goals:

- To the fullest extent possible, sensor networks should be populated by compact, low-cost, minimal care, automatic detectors.
- The network software should be capable of effectively assessing events with heterogeneous arrays of sensors.
- Communications should be able to withstand the peak loads associated with a crisis.
- Computing assets should be distributed and/or embedded, and linked to combined effects, microclimate, and weather/modeling tools for automatic, seamless assessments as events unfold.
- Automatic alarms should be backed up by online modeling and confidence measures.
- Standardized, common lexicon and data formats to afford universal access.
- The network should provide a space-time map of the event, to include parameters such as severity, duration, and population exposure.

Current Capability:

- There are really no operational responder networks for homeland defense. Some experimental networks have been implemented for military force protection by the U.S. Army at CECOM. Although there is much to learn from these efforts, they must be adapted to civilian emergency responders' operations. Furthermore, they need to be expanded to the full CBRNE threat spectrum and scaled up to deal with large urban settings.
- Few commercial buildings have any type of CBRNE sensors and associated network infrastructure.
- Most COTS and GOTS sensors require some adaptation to make them suitable for flexible insertion into networks.

State of the Art:

Technologists have identified many relevant programs, although at this time none will meet the needs of civilian responders without significant scaling and expansion to the full threat spectrum.

Biowatch is a new federal program that involves the DHS and Environmental Protection Agency (EPA). It will modify and use the EPA environmental sampler network to monitor urban environments for aerosol bio-attack. At least 25 cities will be involved.

For the Unconventional Nuclear Weapons Defense (UNWD) program, DTRA has installed experimental, operational nuclear protection networks at four DoD bases. Though limited in scale, they have identified the essential ingredients needed for defense against both nuclear weapons and dirty bombs. The network at Camp Lejeune, NC has also shown how civilian and military responders can be unified to combat this threat.

The DHS successor to the Bio-Defense Initiative, the Bio Threat Consequence Management (BTCM) effort, will fund R&D in a variety of sensor and network integration issues; BTCM results will be useful to the ultimate goals of DIDA.5.

NASA has created a Smart Healthcare Management System, a network of sensors and computers which monitors both environment and personnel status.

NSOF (Network Sensors for the Objective Force) is an Army CECOM R&D effort to support deployments of Unattended Ground Sensors (UGS) networks. The purpose of this project is to develop, provide, and demonstrate communications networks that can successfully interconnect with UGS networks within a sensor field and also connect the UGS network field back to higher-level data fusion and Command and Control (C^2) elements.

Smart SensorWeb, a DoD program, pioneered the concepts of complex integrated networks for the individual combatant. This lower echelon

perspective makes it a useful case study for the responder.

Lawrence Livermore National Laboratory is involved in two programs of interest: the Wide-Area Tracking System (WATS) for detecting and tracking a ground-delivered nuclear device; and the Joint Biological Remote Early Warning System (JBREWS) for alerting U.S. field troops of an attack with biological agents. Both systems consist of a network of sensors and communications links with information continuously evaluated by unique data-fusion algorithms. The sensors can be permanently deployed at chosen locations or mounted in vans for deployment on demand to protect specific areas for specific situations or events.

The Joint Warning and Reporting Network (JWARN) consists of software and hardware components that link NBC detectors to tactical communications for NBC warning, reporting, and battlefield management. This network is being designed for dynamic combat operations.

Finally, the Joint Service Installation Pilot Project (JSIPP), is a DoD program managed by the Defense Threat Reduction Agency; it is designed to upgrade nine military installations to be model sites for biological and chemical safety. JSIPP will be linked with existing responder networks and ESSENCE – The Electronic Surveillance System for the Early Notification of Community-based Epidemics. Ultimately, up to 200 bases may be outfitted with similar equipment under the more comprehensive Project Guardian managed by the military Joint Project Office for CB Defense.

Technology Limitations and Barriers:

The construction of large sensor networks is an engineering problem. No particular barrier exists that must be overcome in order to meet the goals of this element.

Although there are many laudable efforts underway to evolve toward a unified CBRNE sensor network, these efforts do not provide a complete package suitable for homeland defense.

- Military efforts concentrate on defense within the confines of military bases or dynamic combat and do not normally address the needs of large population centers. But some of the results may be scalable to urban scenarios. Furthermore, funding constraints have limited efforts to single threat or small experimental efforts that do not cover the full threat spectrum.

- Modeling software for embedded networking is not seamless. Combined effects modeling is not available, and the outputs from single models are usually fed by hand to another model. Microclimate predictions are needed but are not mature; this problem must be studied in the context of large sensor arrays.

- Current networks and associated software tend to be rigid, hardware specific, and difficult (expensive) to upgrade to new sensor hardware. Networks are susceptible to cyberterrorism, but also fail on their own.

- Communications become overloaded easily.

Gap Fillers:

A major integrated approach to CBRNE networks was recommended by the technologists' workshop. Some of the design considerations for an integrated regional network are listed below. Although some of the pieces of an integrated network are mature, the scale of this capability warrants a major initiative. See DIDArto.5 (*Integrated Networked Sensors for CBRN Detection*) and the DIDA roadmap for additional detail. This technology objective stimulated a great deal of discussion about a wide-range of issues, the most important of which are discussed below:

- Standard sensor, communications, and data formats are needed.

- Self-configuring networks with flexible architecture should be adopted from the military.

- The network should be designed to deal with a wide-range of existing and future sensors to include integration with other sensors – intrusion detection, traffic management, public surveillance, and security systems.

- Data fusion and information management over the network.
- The network must use simulation and physical models (buildings, structures) and have a reachback to CDC, medical surveillance, and other databases.
- All methods of bandwidth management and communications stability should be explored. For example, a low-band width, cell phone-based architecture may be a useful layer if it can maintain effective service during peak demand periods associated with a crisis. Smart detectors and sensors will reduce bandwidth. Surge capacity and scalability will be important design considerations.
- Resistance to countermeasures is going to become increasingly important as terrorists become better equipped and more technically astute.
- Data management and archiving will need to be flexible and easily adjusted to deal with changing policies, laws, and operational needs.
- Perhaps one of the most powerful capabilities of the network will be Global Positioning system (GPS)/GIS tracking of dynamic network elements and possibly victims after the event.

DIDA.6 – CBRNE Effects Modeling and Simulation. *The ability to rapidly produce validated dispersal and effects models for urban terrain and building interiors.* Modeling and simulation can provide an effective extension of individual sensors and spatial-temporal analysis of sensor webs data for event discovery or false alarm mitigation. Models may greatly reduce the complexity of response to combined effects resulting from explosions and associated dispersal of agents. Models must include incendiary, radiation, chemical corrosion, blast, shock, and other effects.

Goals:

- High confidence description of hazard dispersal and effects.
- User friendly.
- Reduction in the complexity of response to combined effects.
- Includes: incendiary, radiation, blast, shock and other effects.
- High quality descriptions in an urban environment.

Current Capabilities:

- Military models exist to an extent, but are not available to or fully adapted for civilian responders.
- Many mature models exist for blast and shock but are only invoked when a crisis occurs and the military comes in to provide post-attack analysis.

State of the Art:

Individual models exist for all agents and all likely methods of agent dispersion. Some combined effects models exist for subsets of the CBRNE spectrum. There is, however, no fully integrated, combined effects model for all the agents/threats.

DTRA's Hazard Prediction and Assessment Capability (HPAC) is an example of existing plume models that predict hazards from CBRN weapons and facilities. It predicts exposure information for military and/or civilian populations attacked with CBRN weapons. HPAC also provides exposure information for populations in the vicinity of accidents involving nuclear power plants, chemical and biological production facilities, and CBRN storage facilities/transportation containers. DTRA also developed the Consequence Assessment Tool Set (CATS) that can help field personnel assess the effects of terrorist and natural catastrophes. Finally, the National Atmospheric Release Advisory Center (NARAC) at Los Alamos National Laboratory has a plume modeling for all hazards. A laptop version exists for use by responders.

Similarly, the SPAWARSYSCOM sponsored Vapor, Liquid and Solid Tracking (VLSTRACK) simulates the release and downwind hazard from a chemical or biological warfare (CBW) attack.

DoD has also developed a sophisticated array of blast effects models and associated 3-D structural models that can be used to assess damage to buildings and structures. These models have been used to estimate the details of well-known terrorist bombings (*e.g.*, Khobar Towers, Oklahoma City, the USS COLE) and have resulted in greatly revised and/or more accurate estimates of bomb size.

For interior dispersion modeling, there are commercial air flow models that can predict air flow inside buildings. Another example comes from the Environmental Protection Agency's Office of Research and Development, which is attempting to develop accurate models for use in urban settings (*e.g.*, "urban canyons"; emphasis is on dispersion of TIC and CB aerosols).

Technology Limitations and Barriers:

The technologists determined that there is a need to combine the existing and emerging models for the separate CBRNE effects into a system of models that can seamlessly provide the best model for the particular scenario at hand. They also noted that there are competing models for the individual threat domains.

- Models are stove-piped into specialty fields due to the limited budgets, difficulty of the science, and missions of developers. Integrated, seamless modeling and simulation of the full range of CBRNE requires the patching together of several massive computer codes.
- Fixed and dynamic sensor networks and robotic sensors are needed to provide information necessary to get reliable results on limited space and time scales (*e.g.*, microclimate data) that can support responders. Results will be highly dependent on the size and latency of sensors.
- Much effort is focused on aerosol models, however some models are needed for indoor, fire/incendiary, structural analysis, and water distribution (DoD and DoE are working on these issues).
- The aerodynamic flow around buildings and in urban canyons may pose a significant challenge to current physical models and scientific understanding of the problem.

The speed of processing and sensor array density will determine accuracy and relevancy for responder use. Modeling of aerosol dispersion in complex urban environments is a matter of current research. Without dense weather sensing and large sensor arrays, the outputs of the individual and combined models may be of little use to the responder on the scene (although responders at higher echelons may find coarse information useful in planning). Accurate pictures of cloud dispersal may not be possible until the weather and sensor infrastructure can support it.

Gap Fillers:

A host of important considerations were identified by responders and technologies. See DIDArto.6 (*Combined Effects Modeling for Urban Canyons*) and the DIDA roadmap for additional details.

- Validation is an essential ingredient. The workshop recommended that greater emphasis and adequate funding be devoted to validation exercises; this includes more simulant releases or live testing in controlled environments. Validation *in situ* is a credible option. DoD and DHS need to closely coordinate validation efforts.
- Models must incorporate 3-D inputs and outputs for cities.
- Microclimate modeling is needed down to meters and five minutes. Compute time should be an important design consideration. If a model needs more time than the phenomenon it is predicting then it will be generally less useful to the responder.

- Responders would like the outputs to be in terms that are familiar to responders, rather than scientists and engineers.
- Responders are very interested in ease of training and certification, and would like to have virtual training capabilities built in.
- Models of operational effects and virtual prototyping can be included, which show the impact of increased capability on overall response.
- Technologists suggested that sensor array density may be an effective way to offset model complexity (*e.g.*, climate sensors vs. climate model, or building stress sensors vs. model complexity). Sensors could track microweather or directly measure agent dispersion. (See DIDA.7 (*Collection and Dissemination of Weather and Environmental Conditions*) and DIDA.5 (*Detector Arrays and Networks).*)

DIDA.7 – Collection and Dissemination of Weather and Environmental Conditions.

Responders need *automatic collection and dissemination of real-time weather information so that they can understand and assess the extent of contamination by airborne agents and bombs.* The collection and ubiquitous availability of accurate weather information is essential to the understanding and assessment of outdoor release of agents. The weather information and associated predictive models should include terrain and building effects. Weather data and models should be embedded in all response systems.

Goals:

- Allows responders to establish and shift perimeter(s).
- Linked to predictive modeling (sunlight, temperature, humidity, wind effects on particular agents).
- Includes interior and exterior micro climates – terrain and building effects.
- Embedded in all response systems.

Current Capabilities:

- Weather and pollutant sensor networks exist but are not fine-grained enough for urban settings.
- They are not integrated with agent characteristics and predictive effects modeling.
- Deployable networks for forest fires exist but are not widely proliferated and not oriented to CBRNE.

State of the Art:

Technologists noted that there were already large investments in weather effects modeling; it was determined that the technology is relatively mature. The DoD alone invests about $160M per year in environmental monitoring, models, climate, and microclimate R&D.

Weather simulations are becoming increasingly accurate and DoD uses weather predictions as a key part of its combat planning for both long- and short-term decisions. Large computers are being networked and employed to provide local weather on demand around the nation.

DTRA has developed a prototype of its aerosol dispersion model for urban scenarios, called Urban HPAC, which uses meteorological inputs. NOAA has efforts to provide microclimate data sensing and modeling including urban microclimes.

Technology Limitations and Barriers:

This is an engineering problem. The cities must determine what weather monitoring infrastructure will best suit their needs and provide the level of weather knowledge and timeliness within their budget. They will need to weigh this against their needs to detect and understand terrorist attacks that depend on weather effects. Some of the effects of weather may be offset by operational plans that minimize the uncertainties associated with understanding weather.

Generally, except for microclimate scale predictions in urban scenarios, this technology is quite

mature. Predicting scales below 1 km will require finer sensor grids and computer simulations that handle the associated increase in data. It is unlikely that the National Weather Service or other civilian needs will rapidly move in this direction.

Gap Fillers:

Since the weather is essential to predicting the dispersal and effects of the agents, the technologists determined that the microclimate gap in this DIDA should be incorporated in DIDArto.6 (*Combined Effects Modeling for Urban Canyons*), and that the sensors for fine scale meteorological data would best be covered in DIDArto.5 (*Integrated Networked Sensors for CBRNE Detection*). Further, the need for integrated effects modeling was felt to be a compelling umbrella that would support a healthy investment in microclimate modeling. See the DIDA roadmap for details.

DIDA.8 – Pre-Triage/Differentiation Among Levels of Exposure. *The ability to integrate sensor information, personal history (pre-exposure and location during event), and physiological symptoms to provide on-scene assessment of low-dose exposure and assists responders in predicting near-term health status and treatment modalities for victims and involved responders.* While at the complex scene of an ongoing or recent event, responders need to guide the removal, expedient decontamination, and preliminary treatment for most critically injured/exposed. They must determine the disposition of the injured and the apparently unharmed. This capability will integrate on-scene sensor readings and any available information on victims' history to determine near-term health status. For example, smart cards carried by the responders would be useful in assessing their condition. Handheld devices may detect whether a victim is in shock or is exhibiting symptoms associated with low-dose exposure to chemical weapons or other toxins and agents.

Goals:

- Remote bio-systems analysis (*e.g.*, responder outside hot zone assessing victim inside).
- Handheld sensors for noninvasive assessment of patient shock (thermal imaging may allow rapid screening of shock and other injury).
- Smart cards with responder health history.
- Linked to sensor readings.
- Non-contact methods are preferred.
- Integration with UIC.1 (*Point Location and Identification*) for responder location history and perhaps physiological status.

Current Capabilities:

- Some laptop data is available, providing information on symptomology and course of illness following exposure, but it is not widely deployed and does not integrate sensor information or personal history.
- Some fire/EMS vehicles carry medical care protocols, but they are in hard copy and cumbersome.
- There are no sensors or instruments coupled directly to computers to provide automatic assessment. Responders must have considerable skill in interpreting data.

State of the Art:

There are pieces of this that are quite mature. For example, diagnosing burn severity in the field is a well developed discipline. However, understanding non-lethal exposure to CB threats and combined effects is still a matter of research. It will take years to develop field deployable protocols and sensing tools that can permit a responder to rapidly distinguish triage cases from others, and act with confidence on the assessment. This element is complicated by legal and privacy issues, which may pose fundamental barriers to the technical solutions. For example, it may be years before the general populace is comfortable with a smart card that contains personal medical history.

The DoD is developing technologies for military medical use that have application to responders' missions: these technologies are being geared for

early detection and assessment of pathogens in the patient's body. For example, the DARPA Advanced Diagnostics Program is developing technology to detect the presence of infection by any pathogen in the body or in prepared samples—in real-time and in the absence of recognizable signs and symptoms, when pathogen numbers are still low. The Army Telemedicine Program has been investing for years in on-scene technology for assessment and treatment of injuries in combat scenarios. This work has established centers, software, sensors and tools that can help field medics rapidly treat certain injuries in the field. The effort has focused on WMD as a major objective. Furthermore, Digital Area Thermography is being studied as a means to assess the effects of blister agents, and gene chips are being developed for rapid analysis of saliva, blood, and sweat.

Technology Limitations and Barriers:

- The physiological observables have not been defined. Are they unambiguous? Can sensors detect them?
- There is a major psychological issue that must be addressed – does shock negate the feasibility of such diagnostics?
- Affordability.

Gap Fillers:

The technologists and responders identified a set of important features that this capability would need in order to be useful:

- Demonstrable physiologic changes – basic research program.
- Non-invasive.
- Capable of detecting early stages.
- Ability to recommend treatment commensurate with level of exposure.
- Must be able to handle many cases rapidly.
- Physiological sensors.

Achieving these was considered very high risk. Thus a research program is recommended; see technology objective DIDArto.7 (*On-scene Assessment of Low-Dose Exposure to Chemical Agents – Research*) and the DIDA roadmap.

DIDA.9 – Rapid Assessment of Structural Integrity/Other Risks (e.g., gas lines). *The ability to rapidly assess and integrate structural information and measurements to allow responders to assess the structural integrity of buildings in the wake of explosions, fires and or impact.* A significant cause of casualties in terrorist events is collapse of damaged structures and buildings. Responders need to know if it is safe to enter and conduct search and rescue. Responders need to conduct post blast/fire/impact assessment of structures and to assess corrosion damage following chemical release. Ideally, tools are needed to make emergency responders act like fast building/structural engineers. This capability will benefit from knowledge of details of specific buildings in advance.

Goals:

- Assists responders in making go/no-go decisions about entering structures.
- Allows responders to act as structural engineers.
- Rapid, compact.
- User-friendly.
- Reliable.

Current Capabilities:

- Motion detectors exist for use in determining structural stability.
- Not everyone has specialized USAR (urban search and rescue) or TSR (technical search and rescue team) equipment and training.
- Data on individual buildings is not available or not rapidly accessible.

State of the Art:

A number of programs exist that provide solutions for various elements of detecting, assessing, or modeling structural integrity or hazards; however, no common suite of tools integrates them into a single capability.

Structural sensors are employed widely in the civilian sector to measure and monitor stress in buildings. Structural vibrometry has become a major development in the aftermath of the World Trade Center collapse. The National Institute for Standards and Technology Fire Research Lab is developing vibrational technologies, used to assess structural integrity under the stress associated with intense heat and fire. Another example of assessment technology is the Multi-Zonal Blowdown Model (MBLM), which calculates the propagation of vapor from a source within a building, described using the Building Model Generator (BMG), with damage described by Munitions Effectiveness Vulnerability Assessment (MEVA), and includes the capability for modeling the release of gas from a vent or aperture in the building.

Radar technology is being developed to assist structural integrity assessment. Los Alamos National Laboratory has developed microimpulse radar that could be used at close range to assess stress and incremental movement of structures after a blast has occurred. This technology holds promise for penetrating a few feet of dry rubble, and walls of standing structures. Also, ground penetrating radar is being looked at by industry for oil exploration, and by the military for mine detection and underground structure assessment.

Other approaches exist for using modeling technology to assess structural integrity and the effects of various stresses. For example, Idaho National Engineering Laboratory has created a large test facility for testing structures in earthquakes; it is a shake table for large structures. Also, as mentioned earlier, DTRA has invested for 50 years in blast modeling and blast mitigation technology. There are numerous tools available through this work. The Bomb Damage Assessment (BDA) Programs within DoD have extended modeling and sensor ideas in recent years as deep, hard targets have become a target of interest.

3-D laser imaging has become a preferred tool for both commercial and military in the measurement and modeling of buildings and vehicles. It can be used to create 3-D wire frame models of structures. Comparisons are easy using change detection software, thus enabling rapid and accurate structural change assessment.

Technology Limitations and Barriers:

This is a very difficult problem but many aspects of it have been studied persistently throughout several decades. Rapid assessment of existing, standing, instrumented structures and buildings is mature, but understanding severely compromised structures and collapsed structures requires more advanced technology. Providing these technologies will require several years of R&D to combine real-time sensing with modeling, to give responders a capability by which they can confidently decide whether a structure is safe to enter. Operational necessity may of course override the recommendations of the technology. Sensors and models exist, but combining them into an on-scene capability will require a sequence of field experiments and model validation cycles to make a useable package.

- There is a lack of high resolution models and sensors and modeling in 3-D for tall and deep structures and ruins.
- Real-time imagery through rubble and walls is a major challenge; viable techniques should look for alternatives to such sensors until they can be made workable.

Gap Fillers:

Technologists noted the existence of many capable models and simulations that are continually undergoing improvement. They also noted that there are excellent sensing techniques that provide static and dynamic stress readings for buildings and structures. They suggested an integration of such sensors and software in a field portable or vehicle mounted package for use by responders. See technology objective DIDArto.8

(*Real-Time Structural Stress Measurement*) and the DIDA roadmap.

DIDA.10 – Remote Detection of Deception/Intent. *The ability to conduct non-invasive, non-contact, detection of human deception and hostile intent at security checkpoints.*
Responders may encounter terrorists prior to or during an event. They need noninvasive, non-contact, tools for screening at security checkpoints where they may use sensors and natural procedures to elicit measurable response associated with deception and hostile intent.

Goals:

- Rapid decisions to avoid congestion at choke points.
- Low false alert rate.
- Reasonable probability (80%) of detecting terrorist.
- Independent of culture and language.
- Based on unambiguous physiological observables.
- Capability of learning and *in situ* validation.

Current Capability:

- There is no sensor augmented capability.
- Responders use intuition and simple interrogation. (Israelis use observation rooms.)

State of the Art:

This capability is in its infancy. DoD is conducting research on close range detection of deception, but the work is in the phenomenological phase.

Technology Limitations and Barriers:

Lie detectors require physical contact. Physiological monitoring of certain human responses (*e.g.*, face temperature profile or eye movement) can be done at useful ranges but tying the observations to an understanding of a person's intent or mental state is a matter of research. Such a capability will need to pass the privacy test, which may pose insurmountable barriers if the general populace places privacy above security. Variability of human response may also doom this element if it is found that there are no reliable indicators, in any combination, that can provide reliable screening. Drugs and conditioning may also defeat the concept. Until unambiguous physiological indicators can be proven to connote hostile intent, this capability will be unachievable.

Gap Fillers:

Technologists and responders could not see this as a credible capability in the near future, but they felt it would be important if the goals could be achieved. An initiative is suggested to develop an experimental data collection and field research capability by 2010. Because this was deemed to be a very high risk effort, it was determined that current DoD efforts should be monitored until 2007; assuming adequate progress, this effort would proceed at that time. See technology objective DIDArto.9 (*Stand-off Automatic Choke Point Screener*) and the DIDA roadmap.

Detection, Identification, and Assessment Response Technology Objectives (DIDArto)

DIDArto.1 – Wearable Integrated CBR Sensors

Objectives:

Develop miniature, seamlessly integrated CBR detectors and collection devices for use on responders, and eventually the general population. Provide rapid (timely) alert to the wearer of danger and type of attack, *e.g.*, proceed to decontamination, administer prophylaxis, take antibiotic, "suit up" or don mask. Provide wireless readout of exposure information, date, time, and location for use in epidemiological analysis, command response, and treatment. The device may be the size of a cell phone and carried in a convenient place that does not hinder free movement, or the sensors may be embedded in headgear and/or clothing and uniforms. The device must have onboard storage and some processing for recording, analyzing, and retaining history of individual's exposure. Also should be capable of

being connected to or integrated with the location/communication devices developed under UICrto.1 (*Point Location and Identification*).

Payoffs:

Wearable sensors will save lives and help responders and leadership understand the extent and severity of population exposure. This will greatly reduce casualties and enable accurate response with minimum panic and confusion.

Challenges:

The detection technologies for CBR are in differing levels of maturity and no programs exist that integrate the three modes. Miniature biological sensors suitable for wearing are in their infancy. The most likely robust solutions involve the use of micro arrays of bio-receptors on electronic readout chips. They are years away from practical field application. Challenges include collection and sampling, receptor design, field life, cost of receptors and associated solutions/reagents, and environmental hardening of the receptors. Developmental chip-sized chemistry labs are now being tested at DoE laboratories. Their false alarm rates and accuracy in complex, "dirty" environments are still in need of R&D. Radiological detectors for wearable sensors are relatively mature, although the device must detect gamma rays and neutrons, and be able to distinguish likely threats from industrial and medical sources. Integration of the three detection modes (CBR) will be a power, size and weight challenge. Reliable alerting, discrimination, and identification are a challenge in this size package.

Milestones/Metrics:

FY2004: Develop and demonstrate biochip technology scalable to unambiguous detection of four agents with consumable costs of $5/day, overall sensitivity (including collector) of 100-10000 (10000 threshold, 100 objective for long-term) organisms for an exposure time of 10 minutes. The limit of detection for biotoxins should be 10-100 nanograms. For handheld chemical detectors, performance goals are a few parts per billion (ppb) sensitivity for nerve agents and 10 ppb for blister agents with a detection time of one minute. Radiation detectors should be improved to incorporate discrimination capability to distinguish common medical isotopes from those used in nuclear weapons.

FY2005: Transition work from DoD and DoE to begin design and development of wearable integrated CBR sensors. Metrics include: total weight of integrated sensor less than 1 pound, battery life of 24 hours, maximum biochip detection cycle of 15 minutes. Demonstrate aerosol sampler with minimum volume collection rate of 12 liters per minute.

FY2006: Verify performance in laboratory and controlled field trials. Show CB modes able to withstand full environmental range. Demonstrate 72 hour operating life of biochip. Neutron and gamma ray detectors should be capable of identifying unshielded nuclear weapon within 10 feet of sensor.

FY2007: Demonstrate integrated devices in responder exercises. Measure false alarm rates of less than 1 per month for each mode in varied urban terrain and conditions. Show effective sensor decontamination process or low-cost to permit disposal of after event.

FY2008: Transition to limited industrial production and deployment with unit cost of $7500 or less in quantities of 1000. Verify transition plan for full rate production price of less than $3500 in quantities of 10,000.

DIDArto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Integrated Wearable CBR Sensors	$0	$15	$30	$20	$10	**$75**

DIDArto.2 – Stand-off Radiation ID

Objectives:

Develop affordable, robust radiation detectors for stand-off discrimination and identification of nuclear weapons and dirty bombs. Processing and sensor must be capable of nearly unattended operation 24/7, and must distinguish between relatively harmless, legitimate sources and terrorist devices. Sensors must be capable of

networked operation and detecting unshielded nuclear weapons in vehicles moving at highway speeds. Deployable nationwide.

Payoffs:

Provides immediate alert to responders and security forces to intercept suspicious containers, vehicles, or objects.

Challenges:

Current radiation detectors are costly, large, and not designed for production quantities suitable for network deployment on a national scale. Primary challenges are: discrimination of threats from legitimate domestic sources and the ability to detect both gamma rays and neutrons in a compact package.

Milestones/Metrics:

FY2005: Transition work from DoD and DoE to begin design and development of combined neutron/gamma ray detector for networked nationwide security applications. Design criteria: range of 10-50 meters; discrimination capability for threat vs. non-threat; physical size <0.3 sq mile area, environmental hardening against weather and temperature extremes; output for network and wireless data transmission; inputs for remote control; and built-in diagnostics.

FY2006: Verify performance in laboratory and controlled field trials. Show ability to discriminate with 90% probability of correct classification at maximum range. Demonstrate ability to detect standard nuclear weapons targets (provided by DoE) at range. Design incorporates resistance to simple countermeasure.

FY2007: Demonstrate prototype devices in responder exercises. Install prototypes at choke points in experimental CBRNE testbed. Demonstrate vehicle performance. Show detection and discrimination at range against moving vehicle carrying unshielded standard target. Vehicle speed <70 mph.

FY2008: Transition to limited industrial production and deployment with unit cost of $25,000 or less in quantities of 1000. Verify transition plan for full rate production price of less than $15,000 in quantities of 10,000.

DIDArto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Stand-Off Radiation ID	$0	$18	$32	$29	$11	**$90**

DIDArto.3 – Integrated Remote Detection of CB Agents

Objectives:

Develop and demonstrate compact, low-cost, reliable sensor technologies and/or systems for wide area, remote detection of airborne clouds and plumes of biological and chemical agents. Such systems should be able to reliably detect and accurately characterize threat aerosol clouds at ranges of up to 1 kilometer. Their field of view should afford area coverage either through wide beam scanning or through point-to-point grids that characterize the transmission path. Use of cloud penetrating sensors or substances is included in this program as an option to provide detailed information about the cloud. These systems should provide real-time data about plume and aerosol paths for use by responders and to feed computer models so that the event progress can be mapped and predicted.

Currently fielded systems are complex, heavy, and large. They are not suitable for deployment outdoors, exposure to the elements, and continuous operation. These limitations need to be addressed.

A key activity for this program will be to transition and reconfigure military technology and concepts to civilian development. Many of the military requirements may not apply to homeland defense, and reducing requirements may lower risk and costs and accelerate maturation. For example, the military avoids the use of bistatic spectral transmission measurements because it cannot predict or control the sensor deployment geometry ahead of time. This constraint does not normally apply to homeland defense. Furthermore, DoD is considering the use of penetrating microrobots and unmanned micro air vehicles to enter a suspicious cloud and collect samples or conduct analysis. It is recommended

that this concept be included in the trade studies for the RTO.

Payoffs:

Allows the emergency responder the ability to detect an attack from a distance, monitor its progress, issue alerts that may prevent contamination of personnel, secure a contaminated area, administer to victims, apply appropriate triage and gather information about the event for evidence collection and analysis. This system is envisioned as part of a layered defense system that either runs continuously or is activated when other systems or intelligence have given an alert to a possible release. The result is the ability to identify a species but not a strain and to enable a course of treatment.

Challenges:

Currently there are no programs that provide combined CB remote detection. The sensors need to be reliable, work in real-time, require no wet chemistry or other exotic consumables and be low-cost. They must be able to detect particles the range of 2-10 microns, and detect aerosolized multiple chemical agents reliably. Chemical detection must deal with both toxic industrial chemicals and chemical warfare agents such as sarin. There is a need for static and mobile sensors that be rapidly deployed to a field location. Low cost upkeep and operational cost are essential for those systems that operate continuously. Some risk reduction may be possible by using fixed bistatic detection grids (transmitter at one location and receiver up to 500 meters away; monitors transmission spectra along path). Computer processing throughput will be an issue for imaging sensors.

Milestones/Metrics:

FY2004: Demonstrate stand-off bioaerosol detection and discrimination range (threshold) of one kilometer, sensitivity (threshold) of 3,000 agent-containing particles per liter of air (ACPLA), and real-time detection. Analyze optimal deployment strategies using modeling and simulation. Study bistatic detection paths for deployment in urban canyons.

FY2005: Transition work from DoD and DoE to begin design and development of remote integrated CB sensors for deployment in urban settings. Adapt technologies to specifically solve homeland defense problem.

FY2006: Continue development working to metrics: range of greater than 500 meters, discrimination of aerosolized biological warfare agents from naturally occurring biological debris, combined false alarm rate of less than one per month.

FY2007: Verify performance in laboratory and controlled field trials. Show ability to withstand full environmental range. Demonstrate 60 degree wide area coverage from single sensor. Show plume detection sensitivity for cloud density of 100 micrograms per cubic meter with 85% probability of detection.

FY2008: Demonstrate integrated devices in responder exercises. Vary sensor deployment based on predictions obtained through modeling and simulation. Experiment with concept of operations. Measure false alarm rates of less than one per month for each mode in varied urban terrain and conditions.

FY2009: Transition to limited industrial production and deployment with unit cost of $25,000 or less in quantities of 1000. Verify transition plan for full rate production price of less than $15,000 in quantities of 10,000.

DIDArto.3 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Integrated Sensor Suite	$0	$25	$40	$29	$10	$0	**$104**

DIDArto.4 – Portable Stand-off Container Inspection

Objectives:

Develop and demonstrate compact, non-contact, non-intrusive sensor technologies and/or systems for detection of biological and chemical agents in sealed containers. Such systems should be able to

reliably detect and potentially characterize threat agents in containers at distances of 1-2 meters. Although emphasis is on the analysis of the vessel contents, a helpful sensing strategy may include detection of unique or suspicious chemical or biological manufacturing residues that may exist on the outside of the container. Current developmental sensors require physical contact with the vessel to function. It is desirable that the sensing mechanisms rely on techniques that are not harmful to humans in and around the vessel. Further, the sensors should be tolerant of viewing geometry if possible. For example, short-range acousto-optical techniques may prove effective. Sensors that require the use of ionizing radiation or high directed energy beams (laser or microwave) may provide utility for scenarios where humans are not near the vessel being scanned.

Payoffs:

This capability gives the emergency responder the ability to detect and possibly characterize the contents of a chemical or biological agent container without contacting the vessel. Stand-off container inspection would permit convenient ranges of 1-2 meters stand-off detection in choke points such as transportation terminals and allow rapid scanning of a collection of objects that may be found in and around the scene of a potential terrorist attack. This also gives responders the information needed to direct attention and focus to specific containers; this could be particularly useful in hunting for terrorist weapons in warehouses and storage areas.

Challenges:

The most significant barrier is the paucity of signatures. Chemical and biological agents are relatively easy to conceal since they emit no radiation, and potent quantities can be carried in small vessels. They do not emit any characteristic observable radiation of any sort. Properly prepared and sealed vessels should not have any unique chemical or biological residues on the surface, although it may be possible to look for unusual amounts of common residues as an alarm to warrant more extensive examination. Containers may vary in size, shape, and composition. It is possible that the agent may be carried in what appears to be a commercial product container or other ordinary object such as a fire extinguisher. The actual agent container may be carried or concealed within another vessel in an attempt to defeat screening. Many detection schemes rely on analysis of fluid characteristics but biological agents are likely to be carried in powder form.

Milestones/Metrics:

FY2004: DoD/DoE to continue development of non-stand-off detection technology for chemical agents. Prove ability to reliably detect selected chemical warfare agents from ordinary harmless chemicals. Determine limits of discrimination capability. Validate useful performance metrics: ability to detect four or more specific chemical agents reliably and distinguish them from ten different harmless fluids with a false declaration rate of less than 10%. Show results against a variety of common fluid vessels such as soft drink bottles, fire extinguishers, and household chemical containers. Extend experiments to consider easily implemented countermeasures that terrorists would consider using to avoid detection.

FY2005: Extend chemical vessel inspection technology to non-contact methods. Show ranges of 10 to 50 centimeter with detection of one or more selected threat chemicals. Assess practical and theoretical limits and define metrics. Develop geometry insensitive inspection techniques for chemical vessels. Define potential techniques for bio-agent vessel inspection: consider bistatic (two point sensing) measurement procedures and associated geometrical constraints for noncontact inspection at busy choke points; examine potential for monostatic (single point sensing) active techniques that can probe the vessel to detect the agent; develop stand-off surface inspection techniques that identify tell-tale residues of substances associated with production or handling of bio-agents.

FY2006: Demonstrate non-contact chemical inspection performance equal to contact methods. Develop compact, portable device, preferably handheld, for stand-off inspection of

chemical vessels. Extend range to two meters or more. Conduct lab experiments of biological vessel inspection technology for promising techniques. Begin development of screener that relies on residue detection on the surface of CB vessels.

FY2007: Demonstrate biodetection: one kilogram of 2-4 selected agents stored in dry form in sealed containers at a range of 10-50 cm. Conduct demonstration against 5-10 commonly occurring commercial or industrial dry containers safe enough to contain biological agents without leakage; *e.g.*, powdered herbicide or insecticide containers (other methods are more reliable for detecting unsafe transport). Conduct operational tests of chemical stand-off inspection devices in rigorous, controlled trials and relatively unconstrained urban responder exercises. Demonstrate CB residue screener detection range of two meters against 3-5 likely residues; identify likely screener confusers and legitimate vessels that would have identical residues.

FY2008: Transition chemical stand-off detector to limited industrial production and deployment with unit cost of $4,000 or less in quantities of 1000. Verify transition plan for full rate production price of less than $2,000 in quantities of 10,000. Deploy CB residue screener in industrial production with same costs.

FY2009: Demonstrate non-contact bio-agent inspection performance equal to contact methods. Develop compact, portable device, preferably handheld, for stand-off inspection of suspicious containers. Extend range to two meters or more. Begin design of combined CB stand-off inspection device.

FY2010: Develop and test CB non-contact inspection device. Show performance of each mode equal to the performance of individual detectors.

FY2011: Transition CB stand-off detector to limited industrial production and deployment with unit cost of $8,000 or less in quantities of 1000. Verify transition plan for full rate production price of less than $4,000 in quantities of 10,000.

DIDArto.4 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Combined Stand-Off CB	$0	$20	$30	$30	$20	$30	**$130**

DIDArto.5 – Integrated Networked Sensors for CBRNE Detection

Objectives:

The ability to defend cities against large scale attacks will ultimately depend on integrated networks of sensors.

- Develop two or more large-scale urban networked sensor testbeds to support the full spectrum of DIDA functions; testbeds should be chosen to cover different urban settings, *e.g.*, a complex seaport environment and a large inland urban complex. Employ arrays of static, mobile, and remote sensors for intercepting nuclear and radiological weapons, detecting and characterizing aerosolized CB agents, and mapping the attack and ensuing effects. Integrate sensor networks with information networks for flow of raw data, indications, and warning. Employ a variety of networked software agents to provide image and data processing, embedded model based detection, false alarm reduction, and event mapping and prediction.

- Support the activities associated with a spectrum of emergency responders, *e.g.*, fire, police, rescue, emergency medical teams and municipal departments. The capabilities include the necessary infrastructure to support communication, sensing, surveillance, instrumentation and data collection for a wide-range of experiments, demonstrations and exercises. The underlying architecture should be scalable and support standard interfaces and connections to facilitate plug and play experiments with systems and sub-systems and insertion of advanced components and technologies.

Payoffs:

The program will establish a national capability for municipalities and metropolitan areas to participate in experiments, demonstrations, and evaluation activities. It will provide an *in situ*, real-time environment for advanced systems and new technology evaluation. The instrumentation and information displays will enable observation of operations spanning multi-threat attacks. It will allow regional coordinators, incident commanders, and emergency responders to train, and experiment with new concepts of operation.

The testbed and associated infrastructure will empower the civilian community to conduct exercises analogous to those conducted on the Western Test Range by the military community. These exercises have proven to be invaluable to military units which subsequently are deployed to a wide-range of countries.

Challenges:

A major challenge is to design the sensor network to overcome the failings of the available CBNRE off-the-shelf sensors. A technical challenge is the testbed architecture which must be scalable and capable of accommodating a wide-range of equipment and systems. A managerial challenge is that a broad set of capabilities is needed, and must be realized through the creation of large industrial/academic teams allied with DoE and DoD laboratories. The sensor network will need to integrate multiple legacy systems as well as state-of-the-art equipment and information systems and data analysis.

Milestones/Metrics:

FY2004: Initiate competitive program with multiple awards for urban sensor networks. Contractors conduct a detailed assessment of alternatives using modeling and simulation, and other analytical tools. Determine cost drivers and CONOPS for sensor networks. Qualified teams will consist of sensor and network firms with expertise and products that cover the full CBRNE threat spectrum. Determine area coverage, population coverage, response time, tolerable false alarm rates, and other key parameters vs. number and type of each sensor. Estimate acquisition and operational costs for two alternative sensor network designs.

FY2005: Complete detailed design of networks. Support Red Team activities for initiating incidents and evaluating real-time response of systems and responder organizations. Begin installation in selected urban centers. Conduct trade study of climate sensor density versus modeling accuracy; adjust climate sensor mix accordingly. Demonstrate initial functional capability to regional coordinators, commanders and emergency responders. Integrate CBRNE sensors and detectors with other commonly used intrusion and security systems to include seismic, acoustic, motion detection, video surveillance, and smart tags. Consider active and passive geolocation and tracking of vehicles, especially in higher risk areas such as shipping centers and ports. Consider implications of tracking victims in response and recovery phases. Employ wireless and wired data transfer as needed. Consider dedicated response networks that do not become overloaded in a crisis.

FY2006: Begin series of spiral development experiments in a networked testbed environment. Develop test plan that provides realistic results without the need for agent release. Support experiments, equipment T&E and training of other metropolitan communities who deploy to the testbed. Demonstrate network false alarm rate of less than one per month with probability of detection of 99% or higher for radiological and nuclear threats. Response time for nuclear weapons attack must be less than five minutes.

FY2007: Demonstrate network false alarm rate of less than one per month with probability of detection of 85% or higher for CB attacks. Show network capability to reduce false alarms by a factor of five over single sensor approach. Continue the development and implementation of the testbed and demonstrate metropolitan scale experiment capability. Support training of coordinators, commanders and emergency responders. Support planning of large-scale exercises and technology evaluation and transfer.

FY2008: Continue support of planning, training and exercises for other metropolitan areas and municipalities throughout the country. Develop transfer package to regional defense. Disseminate and provide indoctrination seminars to states and regions.

DIDArto.5 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Civilian Regional Networks	$100	$150	$200	$150	$50	**$650**

DIDArto.6 – Combined Effects Modeling for Urban Canyons

Objectives:

Integrate CBRNE effects models and simulations for complex urban canyons. The models must include unified, seamless software integration of the most mature and well validated models for CB aerosol dispersion in urban environments, munitions effects, structural damage, thermal damage, blast and overpressure, coupled with microclimate prediction and fine grain climate sensor grid. In addition, they should provide inputs and outputs to help in medical and population monitoring data, as well as provide inputs to models associated with injury and casualty assessment (DIDA.8 (*Pre-Triage/Differentiation Among Levels of Exposure*)).

Payoffs:

Additional capabilities provided to responders include: tracking and prediction of plumes associated with CBR aerosol dispersion in urban settings; integrated modeling of explosive and incendiary effects combined with NRE threats; coupling of transport with damage and expected casualties; and recommendations for courses of action and prediction of population exposure.

Challenges:

There are reasonably validated, existing and/or emerging models for large-scale climate effects for most threats except biological. Current effects modeling efforts are just beginning to deal with combinations of effects, and the microclimate effects encountered in cities still remains an area of significant difficulty. Microclimate models may not become feasible until dense meteorological sensor arrays are deployed. Validation testing and evaluation and testing is a major challenge and technological solutions are being sought to mitigate legal, medical, and environmental constrictions while still providing confidence that models are providing useful information. Most models do not speak to each other; uniformity and standardization of inputs and outputs, common validation metrics, and automatic results transfer and data sharing are needed.

Milestones/Metrics:

FY2004: Assume development lead for modeling of combined CBRNE effects. Adapt existing and developmental single phenomena models. Start microclimate study to determine sensor spacing and kinds needed to provide microclimate model inputs for accurate predictions to 50m or less. Consider use of existing urban sensors both for microclimate and exploitation in physical effects models. Adapt DoD munitions effects models to large urban structures.

FY2005: Establish software environment for integrated effects modeling and simulation data handling and results passing. Combine distributed computing concepts with high performance mainframe capabilities. Pass results over high-speed networks so that predictive capability is not vulnerable to single point failure. Conduct tests of microclimate modeling accuracy and a trade study of sensor density and cost versus model uncertainty; adjust accordingly. Combine CB plume models with blast, shock, and radiation models.

FY2006: Verify microclimate performance and determine accuracy limitations based as a function of types of conditions. Integrate microclimate into CBRNE effects models. Employ multiple models for each agent in order to capitalize on strengths of each and for comparisons. Develop urban *in situ* validation strategy to include dispersion of simulants, real and simulated climate sensor inputs, and inputs from existing building sensors (*e.g.*, stress sensors or urban earthquake monitors). Deploy in the two

urban validation testbeds being used for networked sensors. Incorporate sensor characteristics. Create high fidelity digital models of central core and critical locales of two major urban centers: include 3-D models of all major structures down to 30 cm or less. Define plume dispersal test range in urban center.

FY2007: Demonstrate modeling capability in a series of single and multiple event simulations. Show plume tracking to 10 meter accuracy in 5 knot wind with low turbulence; 100 meter accuracy in 15 knot wind and moderate turbulence. Demonstrate end-to-end seamless modeling and simulation online.

DIDArto.6 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Combined Effects M&S	$10	$25	$20	$7	**$62**

DIDArto.7 – On-Scene Assessment of Low-Dose Exposure to Chemical Agents – Research

Objectives:

Research the feasibility of sensor systems that can reliably determine at the scene of an attack whether an individual has symptoms caused by low-dose exposure to a chemical warfare agent. In the event of a chemical attack, not all victims will receive a dose necessary to kill or disable. Some may be injured and others may experience symptoms associated with low-dose exposure.

Payoffs:

Currently there is no unambiguous means for associating physiological observables with low-dose chemical exposure. This research would complement the ongoing limited research efforts in DoD and extend the analysis to toxic industrial chemicals. It would also determine the feasibility of on-scene detection of low-dose exposure and appropriate procedures for handling and treating these victims, if any.

Challenges:

Associating field observable physiological symptoms with low-dose exposure may not be feasible. The large variety of TIC and CW agents that might be employed, possibly in a combined attack, would greatly complicate this problem. Furthermore, not all people will respond the same way and exhibit the same symptoms; some may not exhibit any observable symptoms at all, but nevertheless need treatment.

Milestones/Metrics:

FY2004: Continue research on methods for inferring human injury from exposure to low-dose chemical agents using animal testing, biochemical analysis, and tissue-based experiments. Continue work in analysis of reliable data from industrial accidents.

FY2005: Extend current work in model-based injury related to moderate-dose exposure. Leverage and expand work in long-term exposure to industrial toxins. Infer from chemical similarity, potential damage associated with new toxins, or toxins for which little useful data exists. Examine physiological symptoms that may occur during low-dose exposure.

FY2006: Develop models of average human response to low-dose exposure. Consider use of a variety of sensors to observe the physiological characteristics of such exposure. Expand work in temporary and permanent respiratory damage associated with exposure to low-dose TIC. Extend DoD efforts with CW agents that damage the skin.

FY2007: Catalog the combined external symptoms that may conclusively indicate the exposure to certain classes of chemical agents.

FY2008: Design sensor concepts that can observe such symptoms in real-time.

FY2009: Incorporate sensor concept designs into human response models.

DIDArto7 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Field Observable Indications and Sensors	$0	$10	$10	$10	$10	$20	**$60**

DIDArto.8 – Real-Time Structural Stress Measurement

Objectives:

Develop a portable, real-time stress measurement sensor for continuous onsite assessment of structural safety. After a blast associated with a terrorist event, responders may need to enter structures or rubble without knowing whether collapse is imminent. During rescue and response, the safety of the structure or rubble may change.

Payoffs:

This capability will save rescuers lives in cases where the structure will not support a rescue attempt. Conversely, lives may be saved because a rescue is safely conducted by avoiding unsafe routes, or because an operation is found to be viable in spite of outward appearances. Responders can continuously assess the structural stress of buildings and rubble. If stress exceeds limits associated with materials and design, or changes in stress exceed safe margins, responders are alerted and can exit to avoid injury.

Challenges:

Structural integrity models work best with detailed information. Such information may not be available for the damaged building; further, detailed information of rubble cannot be obtained rapidly or accurately. The correlation of real-time, continuous measurement of stress, movement, tremors, vibrations, and other observables must be relied upon to provide estimates of the stability. Use of embedded models with real-time data feeds is a major challenge. Key issues are: determination of characteristic or tell-tale signatures; packaging of multi-mode sensor into portable system; size; weight; determination of sensor location for best results; ease of deployment and use; simplicity of results and recommended responder actions.

Milestones/Metrics:

FY2004: Use DoD and DoE structural models and simulations to urban structures such bridges, subways, tunnels, skyscrapers, and arenas. Incorporate blast and shock models and integrate them with these urban structural models. Capitalize on rapid 3-D modeling work to provide means to create structural models of buildings, facilities, and large segments of cities. Examine sensor suite designs that can provide critical data on the scene to feed models.

FY2005: Integrate models with sensor inputs in portable device that can monitor structures while rescue and cleanup operations are ongoing. Verify performance in laboratory and scale model experiments. Migrate testing to full scale facilities at DoE or DoD. Create scale models if needed. Build and test a portable sensor suite.

FY2006: Demonstrate confidence levels of 70 percent on predictive capability of model plus sensor. Enter limited production and fielding: weight of 30 pounds; stand-off 10 meters or more; automatic operations; alarm relay to responders. Conduct operability evaluation in responder exercises. Deploy and test sensor suit in the field if opportunities occur, here or abroad.

DIDArto.8 – Budget in Millions

Thrust	2004	2005	2006	Totals
On-Scene Indications and Sensors	$20	$40	$20	**$80**

DIDArto.9 – Stand-off Automatic Choke Point Screener

Objectives:

Develop sensor systems that can find and intercept terrorists at choke points (building entrances, airports, etc.) prior to their intended attack, or after an attack as they attempt to escape. This capability could allow reliable screening of suspicious or dangerous people via observation of physiological characteristics.

Payoffs:

This capability could prevent attacks and facilitate the capture of perpetrators, saving lives and money. Terrorists and collaborating individuals can be intercepted before they gain access to their targets. For example, a would-be highjacker would be stopped at the ticket counter even though papers and baggage have checked out.

Challenges:

The primary challenge is to identify a set of signatures and observables that provide unambiguous indication that a person intends to or is already executing a terrorist attack. Humans vary widely in their response to threats, danger, and fear. Physiological observables taken individually may not suffice to drive down the false alarms.

Milestones/Metrics:

FY2007: Extend ongoing federal research to conceptual system designs and operational concepts that minimize false alarms and disruption to choke point operations. Sensor should provide unambiguous measurement of key physiological indications associated with terrorist mental state. Non-contact approaches are preferable. Processing of individuals should take no more than one minute. Although identification of people is not a goal, the processing could benefit from identification or prior knowledge of the individual via national database or local records from prior accesses.

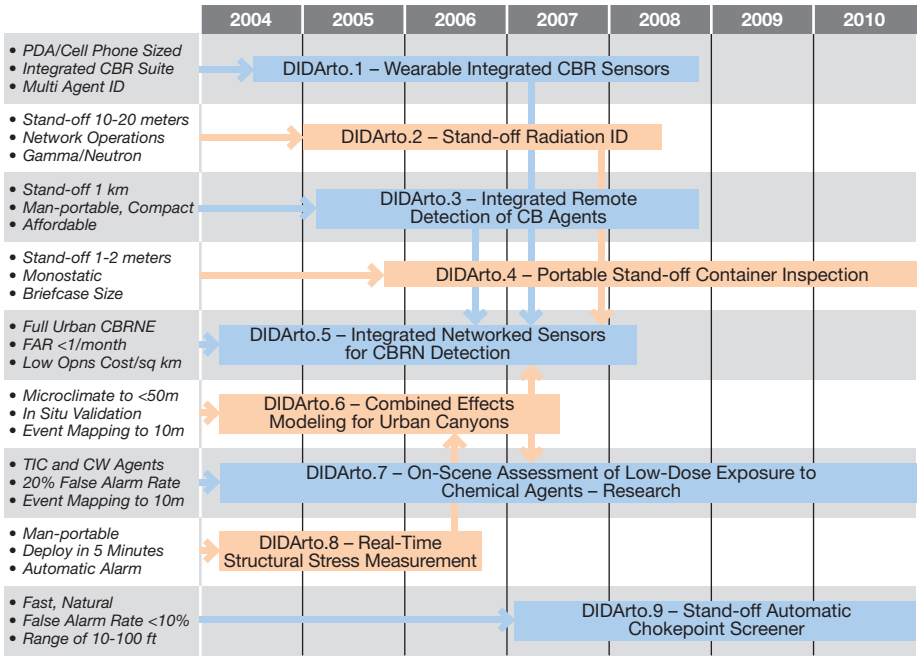
FY2008: Consider the following observables either singly or in combinations as candidates for recognition of intent: voice, gait and head movement analysis, eye movement; odor; temperature; posture changes. Develop concepts that rely on creating a baseline for each individual.

FY2009: Develop operational test scenarios that can be legally implemented in key choke points to collect sensor data. Candidate sensors may include passive and active imaging to include long-wave infrared and eye-safe laser radar, stand-off chemical sensing, and motion sensing, in several spectral regions.

FY2010: Establish test program for competing designs. Use live testing in urban choke points: *e.g.*, airport passenger check-in, ticket booths, building entry, and arena entry. Select most promising approaches based on: accuracy; false alarm rate; throughput or speed of measurement; and cost. Proceed to refined designs in later years.

DIDArto.9 – Budget in Millions

Thrust	2007	2008	2009	2010	Totals
Stand-Off Automated Choke Point Screener	$5	$5	$8	$0	**$18**



Detection, Identification, and Assessment Technology Roadmap

Chapter IV

Unified Incident Command Decision Support and Interoperable Communications (UIC)

Chapter Chair: Dr. Guy Beakley
Chapter Coordinator: Dr. Maria Powell

Definition

Unified Incident Command (UIC) is the capability to seamlessly acquire, store, distribute and protect information needed by the incident commander to successfully manage the response to a terrorism event. "Response," in this case, involves a variety of actions and decisions across police, fire, emergency medical and other departments to include local, state and federal support personnel.

Operational Environments

This capability differs from others in that the functional capabilities do not differ depending on whether the incident is chemical, biological, explosive, or nuclear. Rather, functional elements are evaluated against their performance and contribution to the capability across the spectrum of information management environments which include: Information Acquisition, Information Assessment and Course of Action Development, Decision-Making, and Direction. This means that increases in capability can result from systems integration, engineering, application of commercial-off-the-shelf (COTS) technologies and other solutions not directly reliant on new technology development. For example, organizational changes, equipment/interface standards, and practice/training may be more relevant than technology in solving some of the problems. In addition, some capability gaps can be eliminated by simply procuring devices in large quantities to be distributed in smaller amounts to various jurisdictions. There are some key priority needs, however, that cannot be solved with existing technology or non-technology solutions and will require research and development.

Needed Functional Capabilities and Priorities

The needed functional capabilities prioritized in the Emergency Responders' workshops include the following items, prioritized in order of importance to the responders.

- Point Location and Identification.
- Seamless Connectivity and Integration.
- Information Assurance.
- Incident Command Information Management and Dissemination.
- Multimedia Supported Telepresence.

The responders gave *Point Location and Identification* (UIC.1), and *Seamless Connectivity and Integration* (UIC.2) nearly the same priority but with a slight edge to *Point Location*. The responders believe that the most important piece of information to an incident commander is where his/her personnel and equipment in the incident area are. This is a long-sought after but only partially satisfied need. *Seamless connectivity* addresses the com-munications interoperability issue that vexes most responders when several departments (*i.e.*, police, emergency medical, and fire in multiple municipalities) have to work together in a large event. *Information Assurance*

(UIC.3) and *Incident Command Information Management and Dissemination* (UIC.4) were rated as moderately high but not as high a priority as the first two. Although still considered a needed capability, *Multimedia Supported Telepresence* (UIC.5) was rated the lowest priority among these functional capabilities. The sense of the responders is that there would be real value in having video teleconferencing capability in the field and between responder elements; it's just not as urgent as the other needs.

Unified Incident Command Decision Support and Interoperable Communications

Functional Capabilities	Operational Environments: Information Acquisition	Information Assessment and COA Development	Decision-Making	Direction
1. Point Location and Identification	1	2	3	
2. Seamless Connectivity and Integration	1	2	3	1
3. Information Assurance	1	2	3	1
4. Incident Command Information Management and Dissemination	2	2	2	2
5. Multi-Media Supported Telepresence	1	1	1	1

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

The discussion of the individual functional capabilities addresses the functional needs across the operational elements, as well as technological and non-technological solutions. It should be kept in mind that an extensible framework needs to be put together so that these individual elements can come together and work as a unified incident command. This means, for example, that a solution for point location and identification must work with a solution for interoperable communications in the unified incident command for large and small jurisdictions.

Overall State of Technology for Unified Incident Command Decision Support and Interoperable Communications

The matrix to the right shows a mix of moderate to high technological challenges in raising the level of capabilities for emergency response. However, as the matrix indicates, point location and identification is the only functional capability that calls for technology development with a moderate degree of risk. All other technology areas can achieve results with low technology development risk.

UIC.1 – Point Location and Identification.

This is the ability to know and visualize the location and identity of individual responders regardless of user position or movement, all the time. Safety is a primary concern of the incident commanders. The commander needs to know the location and well-being of each responder for rescue and situational awareness reasons. Point geo-location and identification are necessary regardless of user position or movement. Location information is also useful for giving a picture of where the resources are and monitoring status in cases where the response has a positional objective. For safety it is also useful to measure physiological status of the individual, but cost is a practical concern. A low-cost version of a physiological monitoring system similar to that used by NASA might be appropriate.

Goals:

A key goal is to identify and locate an individual within 3 meters in any direction and under any conditions including weather and interior, within buildings and in tunnels over 400 feet below ground. The responders also indicated that location of high heat and combustion and other hazards (including the chem/bio/radiation hazards as addressed in the DIDA NTRO) would be extremely valuable and should be transmitted by audible alert to the responder in danger and also to a field command location. The positional information, physiological status, (and environmental warning, if provided) must be transmitted

wirelessly inside/outside structures and through rubble to an off-site command post, and to other appropriate parties including within teams of responders. To aid in the visualization of position in the environment, the command display should provide building and other environmental overlays. The command should also be able to provide this information wirelessly back to the responder teams. All this should be accomplished with minimum delay and flawless operation of such a system needs to be assured. The identification and location equipment should come up on the first try and stay up during the entire mission without a "crash" or other service interruption.

Size, weight and power requirements for the remote devices should be kept to a minimum. Power should be provided by small replaceable batteries and should be assisted by an intelligent power/operational management system to ensure that the device would continue to provide essential rescue location service for the duration of a mission, perhaps up to one month. The entire responder package should be smaller than a cigarette pack and should weigh very little more than the battery. It should preferably be integrated into individual protection gear.

Such technology, once available, would revolutionize personnel accountability procedures within responder organizations. All personnel at a response scene, including volunteers, should be equipped with these devices. Thus it would be important that such capabilities either be standardized across jurisdictions and disciplines, or that the equipment has a standard interface to uniforms and personal protective equipment, so that the devices could be issued to all responders entering the perimeter.

Current Capabilities:

Currently there is no affordable system for point location of responders satisfying the above requirements. The requirement, "under any condition" needs to be specified so not to obviate more affordable solutions. An interim goal might be to operate from five stories down in a building or a somewhat more difficult requirement to operate 50 feet down in a subway that has not been previously wired. Responders stated that there is some capability available to locate personnel in the operational area in two dimensions only. Current systems indicate in what direction an individual may be and roughly how far away that individual is, but not, for instance, what floor he/she is on. Current systems are being used mostly by some of the larger fire departments, have limited range and are not integrated into command situational awareness systems. A range of at least 1,000 feet is required.

State of the Art:

Commercial-off-the-shelf equipment exists for a number of applications other than those for responders. These include child location in parks (wristband device placed on the child, receivers at various locations in the park and location stations, where queries can be made), vehicle location systems, Radio Frequency Identification (RF ID) tags for inventory control and various experimental systems. R&D is being conducted on RF ID tags by Naval Air Systems Command and the Army's Land Warrior program, digital RF tags by DARPA/Army CECOM and others, Ultra Wide-band (UWB) by Lawrence Livermore and U.S. Army, and Blue Force Tracking (mostly classified). Army NVESD is presently developing a prototype UWB position location and tracking system specifically designed for interior fire and rescue operations.

The capability to determine the location of a wireless 9-1-1 caller is becoming available in some parts of the country. The FCC's wireless E9-1-1 rules seek to improve the reliability of wireless 9-1-1 services and to provide emergency services personnel with location information that will enable them to locate and provide assistance to wireless 9-1-1 callers much more quickly. Even though this capability does not meet all of the responder needs it will be very cost effective and may be the most satisfactory solution for users with limited resources. The FCC has mandated that wireless carriers provide the geographic location of cellular 9-1-1 callers as part of its E9-1-1 Phase II rules. Phase I of the FCC

mandate, required that, effective 4/1/1998, wireless carriers provide the callback number and the location of the cell site or base station receiving a 9-1-1 call. Phase II of the FCC mandate additionally required that wireless carriers provide the geographic location (*i.e.*, latitude and longitude) of the caller as part of Phase II E9-1-1 implementation, beginning October 1, 2001. The full deployment (*i.e.*, 95% penetration) of this capability is required to be completed by December 31, 2005. The requirements do not satisfy those of the responders in that the location is estimated to within a 50 meter – 150 meter radius for handset-based location technologies, and a 150 – 300 meter radius for network-based location technologies. Also, depending upon the type of location technology chosen by a wireless carrier, a caller's location may not be able to be determined if the call originates from deep within a building or subway.

Steve Wozniak, the co-founder of Apple Computer, recently announced the development of a simple and inexpensive low-data rate wireless network that uses radio signals and global positioning satellite data to keep track of a cluster of inexpensive ($25 production cost) tags within a one- or two-mile radius of each base station. WozNet will include a home-base station that has the ability to track the location of dozens or even hundreds of small wireless devices that can be attached to people, pets or property. While the specific technical solution (reliance on GPS) chosen for WozNet is unlikely to translate directly into the solution for responders (unless high-power GPS pseudolites can be developed to penetrate buildings and rubble), the low-cost of the tags and system suggests that other system concepts could be developed inexpensively as well.

Ultra Wideband is a promising new technology that sends out short pulses that occupy a wide-range of frequency. Because receivers using this technique can discriminate signals in a great deal of noise, transmitters require very little power and the system can operate under the noise floor used by higher-powered devices such as GPS and cell phones. A number of companies such as Time Domain Corp. and MultiSpectral Solutions, Inc. have considerable capability in the new technology, but further R&D needs to be done to meet the responders' needs.

The U.S. Army CECOM has a number of science and technology programs on position, navigation and tracking that directly relate to these needs. One is on advanced position and tracking for the Objective Force and is in its initial year of a four year investigation. Another program uses triangulation technology to pinpoint location within 25 ft. Other programs examine networked assisted GPS, Ultra Wideband (UWB) for ranging, and dead-reckoning models. The Navy uses Infolinks units, which may be too costly for many municipalities. None of these programs meet all of the responders' requirements including low-cost.

Technology Limitations and Barriers:

Point location through 400 feet of ground or concrete is not practical from a size weight, power and cost perspective. Practical ground penetration limits are about 20 feet through r einforced concrete. Going down 400 feet in a tunnel would best be done with a tunnel communications system. It may be best to set an intermediate requirement of penetrating five stories down in a building or a somewhat more difficult requirement of penetrating 50 feet down in a subway that has not been previously wired. Concepts of operations that involve deploying wired links to RF repeaters may help bridge these gaps.

For the near-term the technology risks are moderate to high in propagation through buildings, earth, or rubble, but will likely improve as technologies such as UWB and component miniaturization continue to attain success in performance, size, weight, power, and cost. Barriers to reaching the goals include detection of RF propagation through buildings, walls and rubble.

Gap Fillers:

The chosen approach is to begin with demonstrations of existing technologies combined with research on alternative approaches to surmounting the identified technical barriers and limitations. This initial phase would be followed by

integrated systems development and demonstration and transition to industrial production of the resulting devices.

UIC.2 – Seamless Connectivity and Integration. This is the ability to provide communications systems that are able to seamlessly and dynamically interconnect multiple interagency users (with multiple functions), as well as other information and communications technology systems.

Goals:

Within several minutes after the Pentagon attack of September 11th, emergency workers from ten jurisdictions were on the scene, trying to communicate with different technologies, on different radio frequencies, using different spectrum bands. Incident command communications systems must be able to seamlessly and dynamically interconnect multiple interagency users, who have multiple functions, and multiple information and communications technology systems. The communications system should integrate wired and wireless systems and enable communications within and between tactical, operational, and strategic levels. This includes the ability to support separate communications channels among responders, strike teams and task forces.

A principal problem is that the existing equipment that responders have is not necessarily interoperable among fire fighters, police, and emergency medical personnel, even within the same jurisdiction. This problem has been largely addressed by most jurisdictions, but equipment from different jurisdictions is most likely not interoperable, *e.g.*, the county equipment may not communicate with the city equipment, or adjacent county equipment or the state equipment or various Federal departmental equipment. Interoperability between in-place equipment is a big problem.

Communications capability should include video and data communications in addition to voice. The equipment should be scalable and integrate up to 500 agencies/systems. A call plan with establishment of networks takes care of a lot of problems. 500 people do not need to talk with each other at one time. The system may have to handle that many entities at one time, but even if it were technically possible to allow all pairs to communicate simultaneously, this would not fit with the needs for incident command to maintain a common operational picture flowing up and a coherent set of orders flowing down. There is also the need for responders to spend most of their time doing rather than communicating.

The normal procedure is to establish a hierarchical communications plan that simplifies the connections that need to be made. The system should handle 50 agencies with links to state and national systems. The agencies should have their own network plan with ten or fewer simultaneous callers. The system should not require technicians to be on-site and use common terminology and nomenclature. It should also have the ability to operate within and between challenging environments and terrain, *e.g.*, high rise buildings, underground, in canyons, and on-the-move. A number of levels of security will be required to restrict information that would be harmful in the wrong hands. However, it is envisioned that the security system will be much simpler than that of the military. See UIC.3 (*Information Assurance*). Peer to peer communications in IP networks offers additional capability and should be included.

Current Capabilities:

Communications systems vary across different jurisdictions and departments. Digital communications systems are only just now being deployed across the nation, and for the most part, without concern for interoperability. The standard system in most localities is an 800 MHz trunk system. However, this has limited range, especially in urban environments, and not all localities have changed to this system or have the required repeater system to facilitate its use. The system also takes substantial time to initially upgrade and make available for use.

This is an area where the responders believe that the needed capability, as they have described above, is not available because of a combination

of affordability and lack of standards. There is also a significant deficit in the ability to communicate within large buildings, deep in subway tunnels and in underground structures and canyons. Current systems mostly offer only voice communications, with little or no capability for text, graphics, images, or video.

State of the Art:

Many state and local projects have been instituted for increasing communications interoperability – including, for example, those by the Massachusetts State Police, Kentucky responders and a number of Florida projects, which have been undertaken to relieve the problems in their jurisdictions.

Interconnect appliances exist to interconnect various existing radios. They vary in capability from interconnecting six different radios to interconnecting twelve radios over eight networks.

Standardization efforts have also taken place. Notable among them is Project 25, by the Association of Public Safety Communications Officials, standardized as ANSI 102. Project 25 is an open-standard, digital land mobile radio system that is backward compatible to traditional analog radios. In the digital mode it achieves double the spectrum efficiency and includes packet data services.[8] The problem is the jurisdictions have existing radios and support tower infrastructure and do not have the money to upgrade them.

Wireless network standards include IEEE 802.11 for high bandwidth, packet switched communications but limited mobility due to short-range; IEEE 802.16 for high bandwidth, packet switched, metropolitan area coverage; 3G cellular for medium bandwidth, circuit switched, and continuous coverage via cellular design; and the new IEEE 802.20, which is under development for a continuous coverage cellular system similar to 3G in many respects, but utilizing packet switched access. 2.5G and 3G cellular systems have the advantage that they use the same towers, base stations and radios of the current (2G) digital systems. 2.5G and 3G systems will have data rates of approximately 115 kb/s and 384 kb/s, respectively. Cellular systems are problematic in times of emergency because of the general overloading of the spectrum and potential loss of support structure. However, once effective priority use provisions are put in place, low-cost, and 9-1-1 capability makes cellular attractive for resource-limited organizations.

Emergency responder command and control vehicles are available that offer satellite, software programmable radios, cellular telephone and wireless LAN capability. One problem is the cost (approximately $250,000, although this cost would come down if they were mass-produced).

The Defense Department's Joint Tactical Radio System (JTRS) is a mobile radio system where hardware and software products conform to a single Software Communications Architecture (SCA). The government is procuring a family of affordable tactical radios to meet military communications requirements in a competitive environment by capitalizing on commercial technologies and processes. The radios are expected to cost $2,000 – $5,000 in quantities for one channel and one mode. The SCA makes it possible to procure radio applications such as waveforms and hardware independently. JTRS will be used in the military environment to provide command, control, and communications with forces via voice, video, and data media forms during all phases of military operations to include base support in non-military roles. Commercial availability is expected in 2006.

Power line networks may be considered as a solution to the failure of wireless communications to work in many high rise buildings and under ground. The power line capability should be included in some radios and the radios should work even if the power is disrupted.

Technology Limitations and Barriers:

There are barriers and limitations to solving this problem. One is interoperability of all the different radios that departments have purchased

[8] See Desourdis *et al*, "Emerging Public Safety Wireless Communication Systems," Artech House, 2001 for further information.

over the years. Scale and affordability will be issues here. The requirement for a network manager or technician is also a problem. Two-way broadband communications among vehicles and responders on the move in urban environments is a difficult problem. Interconnection of existing equipment is a solvable problem but upgrades may have to be made in order to meet the requirements. Although the near-term availability of these technologies is marginal, the technological risk of developing them is low.

Gap Fillers:

Because the primary barriers to responders having these capabilities have to do with standards, interoperability (including legacy systems), and availability of resources, the chosen technology approach is to demonstrate a "Responder C^3 System" that is developed over time using a spiral development process. The development should start with the evaluation and adaptation of current off-the-shelf technology and be able to leverage emerging technology as it is developed. This is essentially an engineering effort that establishes standards and an architecture then iteratively incorporates advances in the state of commercial and military technology. The state of the art is moving much too fast on its own to justify adding additional funding into development of the technology itself except in the context of specific extensions of technology for our purposes.

Some of this is already being proposed in the DHS' SAFECOMM program. SAFECOMM is a DHS effort to address the wireless communication interoperability problem for emergency responders at the local, state, and federal levels. It will build on the efforts done to date by the Public Safety Wireless Network Program. The DHS intends to revitalize and enhance the SAFECOMM program however; little information is available about the new program. The SAFECOMM program should result in a national standard architecture for emergency response communications and move toward demonstrating the goals and capability set forth above. Our recommended program leverages the hoped-for results of the SAFECOMM program and establishes a process to continually improve the communications capability of emergency responders.

UIC.3 – Information Assurance. This is the ability to guarantee the availability, confidentiality, security, and integrity of information and information systems, including redundant systems.

Goals:

The unified incident command must have the capability to operate first-time every-time and remain in operation for the duration of the mission. Redundant systems may be required to maintain fail-proof availability. The incident command must provide for security, confidentiality, and integrity of information. The responders see system availability and system integrity as one issue and hence they have been combined under this requirement. The system must have the ability to authenticate users including the device, operator, and data. It must include multi-level security and provide seamless security within and among enclaves and users. The security should, of course, not degrade the data. There should be a visual indication of security status at all levels. The incident command should have monitoring and alert of attempted and actual security breaches. The latency should be on the order of a tenth or a second or less.

Current Capabilities:

Most of the technology needed for information assurance probably already exists, and does not require extensive research and development efforts in addition to efforts already underway. The information assurance issues pertaining to a unified incident command for emergency responders have less to do with technology push than with prioritization of costs, integration of technologies in an incident command system, procedures and non-materiel solutions. Existing techniques from different fields can be applied to incident command.

State of the Art:

There are numerous commercial-off-the-shelf technology options already available or maturing that aid in the authentication of users. Physical security is already fairly advanced through biometrics, digital fingerprinting, facial recognition technologies, and iris recognition. While the technology exists, most of these applications have not made it to the first responder community. For example, there is no authentication on radios in most communities, a potential application would be to use fingerprint authentication on cruiser radios. Currently, user authentication usually comes via an identifier in standard radios, but these are subject to compromise if the radios are lost or stolen. Biometrics is the most favored physical security means, and it is envisioned that biometrics will be in fairly widespread use in the security field for authentication and will be relatively inexpensive (estimate of $25 per unit). A significant challenge will be to define policies that say how the information is shared (by whom, how and when) among the many agencies and entities that may be called upon to collaborate in situations of great urgency.

Authentication of networks can be achieved through Terminal Access Control and Authorization systems (TACAS), Secure ID, Common Access Cards (CAC) and Public Key Infrastructure (PKI). These are all commercially available systems. PKI has become so large that there can be scaling issues with the large number of repository or servers holding certificates, which can increase latency (10 seconds or so).

Currently, there are a number of intrusion detection systems (IDS) that are commercially available that serve as visual identification of security status, *i.e.*, Internet Security Systems (ISS) and Enteyosys "Dragon." Ever since the Linux operating system came out, the Open Source Community Research "SNORT" is the fastest growing IDS system because it is free to companies. However, SNORT can be labor intensive. Organizations should also consider commercial intrusion systems such as those provided by major communications equipment companies such as Cisco Systems Incß.

Real-time video surveillance systems focus on physical security (*i.e.*, force protection against bombs, terrorists, chemical, biological, etc.). These systems have built-in algorithms to identify threats before a security breach has occurred (*i.e.*, snipers, trucks getting too close, employees standing in front of a locked door for more than 10 minutes). As soon as a threat has been identified an alert is sent to central console for processing.

Data Correlation Engines currently focus on Automated Information Systems (AIS) and the areas where people and computers interact. A variety of sensors have been built that provide security to particular areas, *e.g.*, firewalls, intrusion detection systems, and access control servers. Of course, all these sensors generate numerous alerts that could easily tie-up an entire Network Operating Center (NOC) just reviewing them. Data Correlation Engines attempt to reduce all these alerts from many different sensors and make smart decisions to select only those critical alerts that require human intervention. Currently, there are several studies being conducted with regards to the "Insider Threat" to DoD Systems. Some of these studies are proposing the creation of data correlation systems that actually combined physical security systems (video surveillance) with AIS data correlation.

Technology Limitations and Barriers:

Multi-level security system technology tends to be very hard to do and not very conducive to interoperability. Currently, there are "guards" that fit between two different security classification levels on a network. The Operating Systems Multi-Level Security (OSMLS) is one computer that can process both classified and unclassified information. It has been recently developed by DARPA but is not commercially available and is costly. Classified information moving between agencies and especially between Federal and local entities has always been a concern and difficult to implement for both technical and security reasons (many local responders do not possess clearances). It is more appropriate from the emergency responder perspective to have multi-agency security or privacy protection where information

is segregated between agencies that have a need to know about particular information. For example, there may be some criminal information that the police do not want EMS or the Fire Department to know. Also, there is a requirement that 9-1-1 information be kept private. However, the unified incident command needs this information.

Another important aspect when combining different classifications of information is to make sure that it goes to the right database that can store information securely with different levels of privacy. Law Enforcement Online (LEO) might be a good Web-based source/model to maintain secure and local access to pertinent information.

A very high-level of redundancy for all components/pathways/data elements is very expensive and difficult to implement but it can be achieved. NASA and the military services have implemented systems with very high redundancy, but they are very few players in this field. Some amount of redundancy is realistic, but most responder units do not currently have this capability. Most communications channels have two backup routes. Some redundancy is built into cell phones. Nextel phones can become walkie talkies. Most mobile responder units currently have at least two units – a cell phone and a radio.

Less than 1/10 second latency is currently very difficult to achieve especially with encryption. The current state of the art is about 400 milliseconds, but the military have systems with latencies one half that. While responders feel that it is important to have the fastest communications available and intelligible conversations, there is an understanding of what is a reasonable expectation. The marginal improvement in this capability is not enough to justify money to accelerate the current progress of research of improving this technology to less than 1/10 latency.

Information assurance is an area that the emergency response community can piggyback on progress by, and leverage innovation of others. Despite this fact, however, horrendous integration problems and a number of unknown unknowns regarding technologies makes this particular technology marginally available in the near-term. The responders believe little to no capability exists for this element and the technologists believe that the technology development risk is low to moderate.

Gap Fillers:

Again, because the primary barriers to responders having these capabilities have to do with standards, interoperability, and availability of resources, the chosen technology approach is to merge the requirements for information assurance into the overall Responder C^3 System recommended in the previous section. Information assurance technologies are similar to the communication and information technologies discussed in the previous section in that the state- of-the-art is moving forward quite adequately on its own. For our purposes we need to be in a position to rapidly adopt currently available technology and promising new technology as it becomes available. Our recommendation is that the need for information assurance be addressed together with seamless communications. Therefore, we offer a single Response Technology Objective for both areas.

UIC.4 – Incident Command Information Management and Dissemination. This is the ability to provide decision support, situation and resource status management, communication system management, and mission/task tracking in order to allow responders to see, understand and act.

Goals:

The incident command must have tools and services to provide decision support, situation and resource status management, communications system management and mission/task tracking. Streaming video, information visualization, and fusion tools are needed as well as modeling and simulation capability, and graphic representation of geo-location of responders with building/equipment overlay. These tools and services support all hazardous incidents and should be powered from any number of sources including AC/DC, solar and batteries. Commanders need access to all sorts of databases including weather

reports. The decision support suite should have an automated mode where it gives problem alerts without being prompted. The system should operate wirelessly and transmit off-site. And finally the software should have a cost goal of $3,000 to $10,000, which could potentially limit the capability. This cost limit is related to the size of the community – a larger community can afford a more sophisticated system.

The capability should include the acquisition, processing, verification, and targeted distribution of intelligence in operational support of incident command. Real-time access to open source information, *e.g.*, mass media; public safety answering point, *e.g.*, 9-1-1 call data; command board data; and security information is required. Intelligence sources providing imminent threat/danger should provide immediate notification up and down and by push and pull. Tools should be provided for intelligence analysis including data mining, threat/vulnerability analysis, interagency assessment, aggregation, and predictive analysis. The intelligence support should provide the ability to fuse all intelligence disciplines including human intelligence, signals intelligence, electronic intelligence, etc. into one location. Intelligence sources should have priority communications links to the command staff. Provision should be made for automated report generation and information sharing.

Current Capabilities:

This is in an area where the responders believe that technology probably exists, but no one has taken the time or provided the money to integrate technology into a system of systems designed for emergency management unified incident command. They believe there is marginal capability to gather the information necessary, but little capability to manage the information. The responders believe that very little in the way of automated decision support tools is available to this community, and what may be available is too expensive. There is also little data mining capability available to the responders. One of the responders from New York gave this example: a review of emergency telephone databases indicate that at the World Trade Center, 9-1-1 calls came in indicating that the structure was showing signs of collapse in time to warn many of the personnel in the buildings. There was no capability to recognize this or "hotwire" the information to the incident commander and responders.

State of the Art:

Many information management tools are available and emerging to perform incident command and control. In fact the tools exist in many forms and provide varying degrees of decision support, situation and resource management, communications systems management and mission/task tracking. It is true no single integrated system or network exists for performing this function, but programs to set standards and to establish what systems are interoperable would go far toward satisfying responders' needs. In the military, a suite of standards is used to define the parameters to which component modules must conform and this is generally satisfactory toward meeting the goals of information management. For example, the Defense Collaborative Tool Suite sets standards that are used for keeping track of collaboration, chat function, audio, video teleconferencing (VTC), mapping, "white boarding," document sharing, application sharing, etc.

The capability to mine data during an incident is by no means insignificant. Sizable investments have been made by the military on decision support systems with data mining capabilities and these should be leveraged for emergency response operations. U.S. Army CECOM has programs such as DaVinci for distributed analysis and visualization and Area Secure Operations Command and Control (ASOCC) that should be investigated for appropriateness for responders' requirements. DaVinci is a windows-based application that has a map view, a resources view and a timeline view of the emergency event with modeling and simulation and monitoring capability. ASOCC is a package of commercial and government off-the-shelf software that provides information exchange, visualization, collaboration, decision support, and orders and reporting functionality. These systems should be considered for appropriateness in providing

effective information management and dissemination.

TSWG's CoBRA, the chem-bio response aid, is a cost effective application and is available on a ruggedized laptop. However, it lacks resource monitoring and tracking capability. There are a number of other sophisticated systems for laptops such as PEAC (Palmtop Emergency Access for Chemicals) and CAMEO, which have capability to model plumes. At least 50 different software packages exist that provide expert agents, emergency service information management, engineering analysis and decision support. A concerted effort is needed to fully integrate some of these technologies into fully functional systems in the context of responder operations. Efforts should be expended to objectively evaluate systems that show promise and to determine the best of breed for the responders' requirements. The important point is to integrate the best of breed into system of systems and decide the standards, to prevent proliferation of incompatible systems.

Many of these capabilities and some others are being encompassed by the Defense Department's Homeland Security/Homeland Defense Command and Control ACTD (HLS/HD C^2 ACTD). Its purpose is to provide a homeland security decision support center for knowledge capture and knowledge management using high-powered computing and visualization capabilities for emergency response.

Technology Limitations and Barriers:

Although responders believe little to no capability exists for this element, technologists believe that the technology development risk is low, with technology readily available in the near-term.

Gap Fillers:

The program we are recommending leverages the HLS/HD C^2 ACTD to provide ever increasing capability in a spiral development process. It uses the technologies integrated into the ACTD as the basis and then evaluates emerging technologies for inclusion in an Incident Command Informational Management Tool Set. The key to the process will be a constant eye toward reducing cost. The cost of the system needs to be such that local emergency management organizations can afford it.

UIC.5 – Multimedia Supported Telepresence.

This is the ability to provide a multimedia telepresence between incident commanders response personnel, technical specialists, and off-site facilities.

Goals:

The unified incident command should provide multimedia telepresence capabilities among and between incident commanders, response personnel, technical specialists, and off-site facilities including the capability to stream video. This includes the ability to provide an overhead view, to see beyond the current location utilizing such capabilities as manned aircraft, UAVs (unmanned aerial vehicles), UGVs (ground) and national assets such as satellites. Real-time virtual reach-back (private national network) is to be provided. The incident command should provide distributed collaborative decision support capability. It should provide for 5-7 critical feeds and handle up to 100 sites for up to three separate teleconferences. It should have the ability to link with outside entities that are not necessarily on the established network such as CNN by whatever media including phone, video, and web. The multimedia should be scalable and support hand-held capabilities in the field. It should be easily usable and provide good image quality, even if the responder is moving. The system should have the ability to incorporate the appropriate security schema.

This is an area where inexpensive COTS equipment should be employed and adapted where necessary. Being able to collaborate and see from afar is a very powerful tool, but the cost of an implementation can be considerable. Capabilities of the military and intelligence community should be examined to see what fits its requirements. In addition, the command should look to the Internet for practical solutions that can be implemented at low-cost.

Current Capabilities:

Video teleconferencing technology is available and deployed in some areas. For a large number of areas it is simply too expensive for many users. No responder department represented in the workshops had anything close to the above capability desired by the responders. Such extensive capability, to include collaborative decision support and connectivity with handheld devices in the field is not even on the horizon as far as the responders can now see.

State of the Art:

Information portals or gateways are commonly constructed providing access to the Internet for specialized services. A dynamic system can be designed, leveraging Internet methodologies, for *ad hoc* networks that support multimedia services. The architecture can be configured such that systems are separable, but interconnected to maintain privacy. By implementing inexpensive computers and hand held devices each unit (node) can be low-cost and offer considerable power to access information needed by the responders.

The National Guard now has the technology to link up to 100 locations. It is in the process of upgrading its teleconferencing system to one based on the Internet protocol. The Defense Collaborative Tool Suite (DCTS) sets standards that are used for collaboration, chat function, audio, video teleconferencing (VTC), mapping, "white boarding," sharing documents, sharing applications, and optionally streaming media. The Joint Interoperability Test Command tests DCTS equipment for certification. DCTS exceeds the requirement for 5-7 critical feeds now, but the cost of $150,000 per suite may be too expensive for most users. It would be prudent to see if a cost reduced system could meet most responders' needs.

A large amount of research and development work is being conducted in the multimedia area. A new compression technology has been standardized jointly by the International Telecommunication Union and International Standards Organization that permits quality video to fit in half the bandwidth previously required. TSWG is having work done on a Teleconferencing Bridge to develop a secure communication system that allows military and other government organizations to communicate with multiple parties simultaneously in a secure, but not classified environment. The secure bridge sends encrypted communications to up to 30 connected devices. The design will support communications between both fixed and mobile units.

Video technology changes rapidly since it is developed for many commercial applications. Micro cameras exist today that previously did not exist. Games, the Internet, and computers have pushed the technology to low-cost solutions for the home. There are commercial services that offer city maps, 3-D images, building plans, and the like. One example is I3 Systems (3-D imagery, outside the building, modeling, website). The idea is to link to these various services for data mining. Efforts are being made to obtain interior plans for buildings (not through 3-D imagery but by other requested standards). Police have gone into many public buildings and completely mapped the area. Obtaining blueprints of older buildings is generally not a problem, although the accuracy and timeliness of the drawings are many times a concern.

It is desirable to have a common operational picture and be able to click on the area of interest. The Army has a program to obtain and distribute a Single Integrated Ground Picture (SIGP).

Technology Limitations and Barriers:

The only technical barrier noted was the ability to provide such a robust system at a cost that local agencies can afford.

Gap Fillers:

The chosen approach has two phases. The first is to adapt current Web-based technologies to the Responder environment. The second is to integrate this system into the emerging Responder C^3 System and refine these systems through a series of exercises into a standardized package for responder use.

Unified Incident Command Decision Support and Interoperable Communications Response Technology Objectives (UICrto)

UICrto.1 – Point Location and Identification

Objectives:

Conduct demonstrations of existing point location and identification technologies combined with research on alternative approaches to surmount the identified technical barriers and limitations. The demonstrations should be followed by integrated systems development of point location hardware and transition to industrial production.

The system should locate within three meters in any direction, identify, and determine the well-being of each responder under any conditions including weather and interior to buildings and underground.

The point location and identification transmitters should be miniaturized and seamlessly integrated for use on the responders' person or clothing. They should provide rapid (timely) alert to the wearer of danger to well-being and type of attack and wireless readout of exposure information, date, time, and location history for use in epidemiological analysis, command response, and treatment. The device should be smaller than a cigarette pack and carried in a convenient place that does not hinder free movement, or the sensors may be embedded in headgear and/or clothing and uniforms. The device must have onboard storage and some processing for recording, analyzing, and retaining history of the individual's exposure.

Payoffs:

Wearable sensors will save lives and help responders and leadership understand the extent and severity of population exposure. This will greatly reduce casualties and enable accurate response with minimum panic and confusion.

Challenges:

The commanders want a fool-proof system for locating a person in any event, under any conditions, and in tunnels over 400 feet below ground. Point location through 400 feet of ground or concrete is not practical from a size weight, power and cost perspective. Practical ground penetration limits are about 20 feet through reinforced concrete. Going down 400 feet in a tunnel would best be done with a tunnel communications system. We need to further refine the requirement to see if there is an intermediate requirement of penetrating five stories down in a building or a somewhat more difficult requirement of penetrating 50 feet down in a subway that has not been previously wired. Reliable alerting, discrimination, and identification are challenges in a small package that accompanies the responders. The combination of a point location and identification device and well-being monitor makes the wearable device necessarily larger. Key enabling technologies include 3-D visualization, UWB technology, state-of-art battery supplies, miniaturization of electrical components including antennas, and product ruggedization.

Milestones/Metrics:

FY2004: The Department of Homeland Security (DHS)/The Technical Support Working Group (TSWG) initiated a new Broad Area Announcement on Integrated Spatial Recognition that can yield results for this requirement. However, programs are needed that specifically address the responders' requirements. The programs can be segmented into what is available now (principally above ground), R&D on point location in buildings, and research below ground. Homeland Security should sponsor a new program demonstrating current point location, identification, and tracking technology above ground, in a basement underground and under rubble. The Army Night Vision UWB prototype is scheduled for 4QFY04 and could form a baseline for the current state of the art of UWB in interior search and rescue operations. The cost would be about $2 million and require one year.

FY2005: Over the next two years, a second program should be established for R&D for point location within buildings. UWB is a promising technology for this application. The

R&D program would cost about $10 million over two years with a prototype at the end of the program. Metrics include: total weight of integrated sensor, less than one pound and battery life of one week, minimum.

FY2006: The third program is research in what can be done in propagation through the ground, through concrete, and under rubble. This could be a million-dollar-a-year program and could last as long as there are promising new results. The performance should be verified in laboratory and controlled field trials.

FY2007: Battery life of resulting systems should be extended to one month. Demonstrate integrated devices in responder exercises.

FY2008: Implement the point location and identification system and demonstrate it.

FY2009: Transition to limited industrial production and deployment with unit cost of $50 or less in quantities of 1000. Verify the transition plan for a full rate production price of less than $30 in quantities of 10,000.

UICrto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Point Location and Identification System	$2	$5	$6	$3	$3	$2	**$21**

UICrto.2 – Seamless Connectivity and Information Assurance

Objectives:

Demonstrate a "Responder C^3 System" that is developed over time using a spiral development process. The development should start with the evaluation and adaptation, if necessary, of current off-the-shelf technology and be able to leverage emerging technology as it is developed. This is essentially an engineering effort that establishes standards in an overall open architecture and then iteratively incorporates advances in the state of commercial and military technology.

The Responder C^3 System must be able to seamlessly and dynamically interconnect multiple interagency users, who have multiple functions, and multiple information and communications technology systems. The communications system should integrate wired and wireless systems and enable communications within and between tactical, operational, and strategic levels. This includes the ability to support separate communications channels among responders, strike teams and task forces.

The program will also address information assurance needs of first responders. Those needs include the capability to operate first time every time and remain in operation for the duration of the mission. The system must have the ability to authenticate users including the device, operator, and data. It must include multi-level security and provide seamless security within and among enclaves and users. The security should, of course, not degrade the data. There should be a visual indication of security status at all levels. The incident command should have monitoring and alert of attempted and actual security breaches.

The program will leverage the efforts and results of the SAFECOMM program with regard to wireless communications interoperability and will be the integrating activity for all emergency response communications standards and systems. It will also leverage DoD efforts such as the Army Land Warrior, Future Force Warrior, and Future Combat Systems programs, which call for integrated networked operations that involve the dismounted soldier.

Payoffs:

Interoperable communications will save lives and help responders and leadership understand the extent and severity of population exposure. This will greatly reduce casualties and enable accurate response with minimum panic and confusion.

Challenges:

The primary barriers to responders having seamless connectivity and integration have to do with standards, interoperability, and availability of resources. Responders have existing equipment and the equipment is not necessarily interoperable among fire fighters, police, and

emergency medical personnel, even within the same jurisdiction. Interoperability between in-place equipment is a big problem. Developing a national architecture and standards will require cooperation at all government levels and across dozens of non-government organization. This is a huge cultural issue.

Milestones/Metrics:

FY2004: Evaluate the progress of the SAFECOMM program and develop a program schedule to accommodate expected accomplishments. Evaluate military C^3 capabilities for meeting responders' needs.

FY2005: Establish an overall Responder C^3 Systems architecture and standards set capable of integrating the networked sensors of DIDArto.5 (*Integrated Networked Sensors for CBRNE Detection*) using COTS technologies wherever possible. Begin evaluating "off-the-shelf" (both commercial and military) technologies that address the goals described above. Integrate COTS technologies as appropriate into a demonstration system.

FY2006: Begin integration of SAFECOMM results and ICIM tools (UICrto.3) as appropriate. Demonstrate initial capability with available COTS and SAFECOMM developments. Evaluate the demonstration and begin integrating the next block of improvements as indicated.

FY2007: Continue to integrate SAFECOMM, COTS and ICIM tools into the system. Develop and conduct large scale demonstration for seamless connectivity and information assurance capability across at least ten jurisdictions and 20 or more agencies. If possible, piggyback on scheduled emergency responder exercises. Continue to evolve the architecture and standards. Begin the Responder C^3 Systems commercialization effort to increase the likelihood of transitioning the capability to responders.

FY2008: Integrate Point Location and Identification technology developed under UICrto.1 (*Point Location and Identification*) and other improvements indicated by the previous years' demonstration. Continue Responder C^3 Systems commercialization efforts.

FY2009: Complete integration of ICIM and point location tools and transition the demonstration system to architecture and standards maintenance efforts.

UICrto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Responder C^3	$6	$10	$15	$20	$20	$10	**$81**

UICrto.3 – Incident Command Information Management and Dissemination

Objectives:

Provide incident command decision support, situation and resource status management, communications system management and mission/task tracking. This capability should include information visualization and fusion tools as well as modeling and simulation capability. It should include graphic representation of geo-location of responders with building/equipment overlay. It should have access to all sorts of databases including weather reports. The decision support should have an automated mode where it gives problem alerts without being prompted.

In addition, the capability should include the acquisition, processing, verification, and targeted distribution of intelligence in operational support of incident command; real-time access to open source information, *e.g.*, mass media; public safety answering point (9-1-1) call data; and command board data. Finally the software should have a cost goal of $3,000 to $10,000. The effort will be a true spiral development, demonstrating and transitioning increasing progress toward the target capability (as defined by the goals), in increments.

A national DHS SONET (synchronous optical network technologies) digital backbone system is needed to provide the imagery, voice, data, and video information needed. It should be a part of a DHS telecommunications system. Leveraging the DoD's Global Grid as well as a number of existing commercial

communications "rings" should provide adequate technology.

Payoffs:

Incident command information management and dissemination will save lives and help responders and leadership understand the extent and severity of population exposure. This will greatly reduce casualties and enable accurate response with minimum panic and confusion.

Challenges:

The capability to mine data during an incident is by no means insignificant. Sizable investments have been made by the military on decision support systems with data mining capabilities and these should be leveraged for emergency response operations. Making the system of systems extensible going from very low-cost for simple systems to rather high cost in larger metropolitan areas is also a challenge.

Milestones/Metrics:

FY2004: Evaluate the results of DoD's HLS/HD C^2 ACTD. Perform a gap analysis between the DoD system and the goals set forth above. Begin construction of a DHS SONET digital backbone to support the ICIM testbed.

FY2005: Transfer the ACTD technology into an ICIM testbed. Finish construction of a DHS SONET digital backbone system. Evaluate COTS technology to address gaps identified in the previous year and reduce the cost of the overall toolset. Begin developing the initial ICIM tool set with DoD and COTS technology.

FY2006: Complete development of initial ICIM tool set. Demonstrate the capability in an emergency response exercise. Transition the capability to the Responder C^3 System (see UICrto.2 (*Seamless Connectivity and Information Assurance*)). Continue to evaluate COTS and new technology to improve capability and reduce cost.

FY2007: Demonstrate and transition increased ICIM capability to the Responder C^3 System.

FY2008-2010: Continue progress toward target capability and beyond by iterating and transitioning new versions of the ICIM toolset.

UICrto.3 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
UIC Information Management and Dissemination	$15	$15	$20	$7	$5	$5	**$67**

UICrto.4 – Multimedia Supported Telepresence

There are many camera systems in place that may be able to provide information about an incident. The problem is how to collect the video, process it and distribute it. It would be helpful to the incident commander if he/she could plug into a video system already installed in a building. This is a systems access/integration problem as well as a dissemination problem. High resolution in the imagery is a desirable feature. The responders need current images, not those of a week ago. There is also a great need for information that is not readily available at an incident. This includes detailed maps, land-use data, and infrastructure such as airports, railroads, highways, bridges, and utilities. A program needs to be instituted using Internet technologies for obtaining this information on a timely basis. This is analogous to the radio communications gateway discussed in UICrto.2 (*Seamless Connectivity and Information Assurance*), but this is an information portal or gateway.

It is greatly desirable to have an overhead view of the incident. This can be done by tethering cameras or even repurposing a camera system from a UAV such as Predator into a manned system for flying over incident areas. An additional problem exists in transmitting a video from a scene to a responder in route, especially in an urban canyon. On-the-move receivers are needed that work in urban canyons. Metadata (data about the image – where is it, what it is, etc.) is also needed and should be inserted into the video at the source. These advanced multimedia features could be included in an advanced concepts technology demonstration to collect the relevant information about an incident, integrate it, and make it available to the responders. The cost of such a program should be about $2 million with duration of one year. The main risk is

feasibility (user friendly, functional, form factor, and cost). A broader $5 million program should be undertaken subsequent to the demonstration for setting standards over the next three years.

Objectives:

The first objective is to adapt current Web-based technologies to the responder environment in order to obtain multimedia information on a timely basis. The second is to refine these systems through a series of exercises into a standardized package for responder use. The program using Internet technologies will gather low hanging fruit and should cost about $2 million for a first year program to integrate current Web technologies.

Establish an advanced concepts technology demonstration to collect the relevant information about an incident, integrate it and make it available to the responders. The cost of such a program should be about $2 million with duration of one year. A broader $1 million per year program should be undertaken subsequent to the demonstration for setting standards over the next few years.

Payoffs:

Multimedia systems will save lives and help responders and leadership understand the extent and severity of population exposure through actual visualization of the incident. This will greatly reduce casualties and enable accurate response with minimum panic and confusion.

Challenges:

The main risk is feature/function feasibility (user friendly, functional, form factor, and cost).

Making the system of systems extensible for going from very low-cost simple systems to rather higher cost, larger metropolitan systems is also a challenge.

Milestones/Metrics:

FY2004: Develop and demonstrate Internet technologies for obtaining multimedia information on a timely basis. The system should do a quick search in less than one second. It should have drill-down capabilities. A second project should be initiated to establish an ACTD to collect relevant information about an incident.

FY2005: Productize the Internet software. Establish standards based on the multimedia ACTD.

FY2006: Verify performance of the Internet software in laboratory and controlled field trials. Establish standards based on the multimedia ACTD.

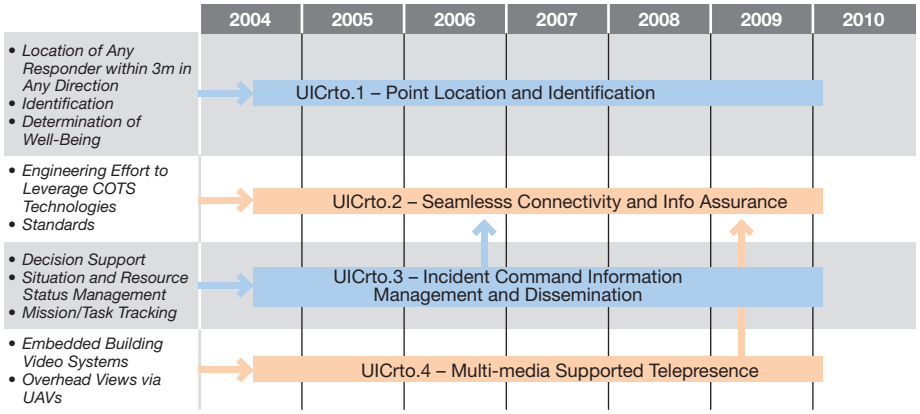
FY2007: Demonstrate the Internet software in responder exercises. Establish standards based on the multimedia ACTD.

FY2008: Transition to the Responder C^3 System (see UICrto.2). Further establish standards based on the multimedia ACTD.

FY2009: Conclude the standards effort based on the multimedia ACTD.

UICrto.4 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Multimedia Supported Telepresence	$4	$5	$3	$3	$3	$1	**$19**



Unified Incident Command Decision Support and Interoperable Communications Technology Roadmap

Chapter V

Response and Recovery (R&R)

Chapter Chair: Dr. Barbara Reagor
Chapter Coordinator: James Hammill

Definition

Response & Recovery (R&R) is the capability for the rapid location and rescue of individuals trapped or isolated by the effects of a terrorist attack, and the rapid, effective and thorough decontamination of large numbers of victims, buildings and equipment, to support emergency response operations to include urban search and rescue, decontamination and restoration of critical services.

Operational Environments

Response and Recovery is focused on the five operational environments represented by the threat: chemical, biological, radiological, nuclear, or high-explosive and incendiary effects of an event. These threats are explained in detail in the Chapter III (DIDA). The effects represented by these operational environments were kept deliberately broad to reflect the variations in capabilities and understanding among jurisdictions of different sizes and resource levels (*e.g.*, volunteer emergency responders in small towns to career emergency responders in large metropolitan areas).

Needed Functional Capabilities and Priorities

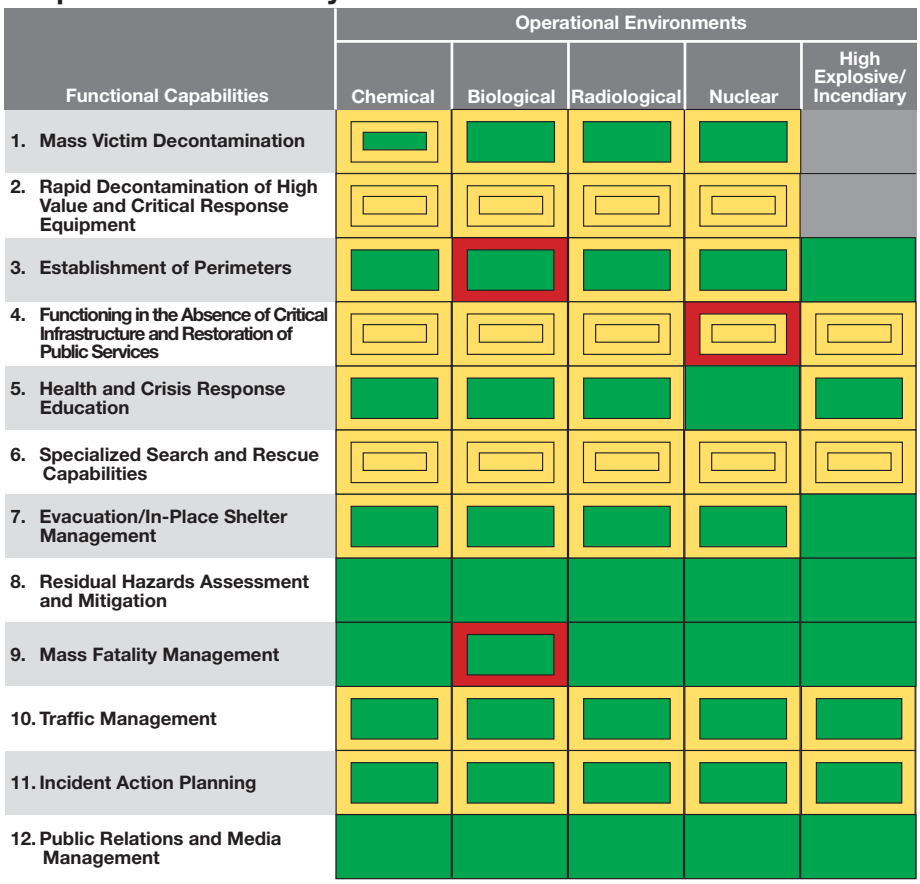
Emergency responders identified and prioritized twelve functional capabilities needed to respond in the operational context and mission statement described above. These capability elements are presented below, in order of descending priority.

- Mass Victim Decontamination.
- Rapid Decontamination of High Value and Critical Response Equipment.
- Establishment of Perimeters.
- Functioning in the Absence of Critical Infrastructure and Restoration of Essential Public Services.
- Health and Crisis Response Education.
- Specialized Search and Rescue Capabilities.
- Evacuation/In-Place Shelter Management.
- Residual Hazards Assessment and Mitigation.
- Mass Fatality Management.
- Traffic Management.
- Incident Action Planning.
- Public Relations and Media Management.

Overall State of Technology for Response and Recovery

The matrix on the next page shows that responders have at least a marginal capability in most of the functional capabilities represented. Furthermore, in those areas where some technology development is still required, technologies can be delivered, or at least demonstrated, in the near-term, without significant technology development risk. This means that capability increases are possible in the near-term in this particular NTRO. It also means that barriers to capability increases are more likely to be related to cost, training, policy, or planning concerns than to technology *per se*.

Response and Recovery



R&R.1 – Mass Victim Decontamination. *The ability to identify contaminated people, isolate them, move victims out of the "warm zone," and remove contaminants at a gross (not definitive) level.* This also includes an ability to determine the necessary level of decontamination required before further transportation or treatment.

Goals:

- The minimum level of decontamination this capability should insure is dependent on the contaminating agent itself, but generally should be a level sufficient that the victims no longer present a secondary contamination risk to themselves, their emergency responder/caretakers, or to the immediate environment. This means victims, once decontaminated, could be handled by responders using only gloves and minimal protective clothing.
- This functional capability ought to be directly supported by, and interactive, with other capabilities that provide real-time information on presence and type of contaminant. This will be dependent on capabilities reflected in Chapter III (DIDA).
- Decontamination "through-put" needs to be scalable to accommodate victims as quickly as they can be brought to the decontamination zone.

Current Capabilities:

- Responders believed there is now a marginal capability to perform this function, limited mainly by cost and availability of equipment.
- This functional capability is stronger now for the nuclear and radiological operational environments than it is for chemical and biological environments, especially for those jurisdictions with nuclear power plants or other significant presence of radioactive materials. This is due in part because of the focus and attendant resources the federal government places on areas with nuclear power plants, weapons labs, etc.; a different focus than the federal government places on chemical storage facilities or plants that process toxic industrial chemicals and materials.

- Responders believed that the high explosive/ incendiary operational environment was not relevant to this functional capability. Although high-explosive or incendiary terrorist attacks can have toxic effects, these effects would be handled as in a chemical operational environment. A large amount of dust and dirt *per se* is not considered contamination.

State of the Art:

The U.S. Government has years of experience in mass decontamination for radiological crises. However, even with this experience, large amounts of equipment are still required to collect effluent during radiological decontamination efforts.

For chemical decontamination, the standard approach is to use mass quantities of water for general classes of chemicals. However not all chemicals can be effectively removed using water. The effectiveness of specific technologies and methods for chemical decontamination will be inherently dependent on detection and identification of the agent. These capabilities can be found in Chapter III (DIDA).

There are a number of programs underway that have application for this functional capability; however, these programs are not necessarily being developed with emergency response applications in mind. Technologists believe there is an opportunity to provide access to some technologies that have been or are under development in the federal government and military arenas. At a minimum, there is an opportunity for technology transfer to assist emergency responders in the short-term by engineering and demonstrating these technologies for emergency responder applications.

Technology Limitations and Barriers:

The primary limitation for fielding these technologies is one of cost, rather than technology. Costs will be especially prohibitive for decontamination equipment that is agent-specific (cost for decontamination equipment for standard toxic industrial chemicals and materials is within reach). Cost considerations also limit training and sustainment of new capabilities for mass victim decontamination: the drain on personnel and resources for training on new technologies and products transferred, for example, from the Defense Department to the local response community will require ongoing funding to assure proficiency and maintenance is sustained.

Technology is marginally available in the near-term for chemical decontamination. Responders and technologists agreed that many chemicals can be cleaned with existing or near-term technologies for certain chemical agents (mainly military chemicals). However, generally applicable technologies are only marginally available in the near-term, that would adequately perform in an environment where military-grade and/or toxic industrial chemicals/toxic industrial materials (TICs/TIMs) were present in mixes. It was agreed that one can rapidly determine presence of general classes of agents, but the specialized equipment tends to be built around chemical warfare agents, and is expensive.

A technological limitation of decontamination technology is one that is also inherent in detection and identification technology: minimizing false positives in detectors, swipes, etc. Current detection equipment requires specialized labor-intensive maintenance in order to keep error rates down.

Finally, decontamination effectiveness will be limited by the ability to contain or neutralize contaminated effluent. EPA guidelines have not adequately addressed the release or disposal of contaminated run-off. Emergency responders will not have the luxury of waiting for a decision. A "mass decontamination effort" will require immediate action and the decision will rest with the incident commander. An interim solution at the scene may be to collect effluent in lots of barrels or pumped into large tank trucks or bladders (if available) and hold for disposition. This would require tracking of the containers.

Gap Fillers:

Technology advances in this area are considered to be of low technological risk and achievable in the near term. Technology programs must first differentiate civilian needs from military, and

then consider existing military equipment and technology to transition to responder use (including mobile detection mounted on vehicles). The DoD's Office of Technology Transition (Commercialization and Dual Use Science and Technology divisions) should be engaged to see where technology exists and whether it can be moved to the private sector for commercialization and/or transferred to the emergency responder community through technology transfer.

In tandem with investigating current programs, the U.S. Government (ideally, the Department of Homeland Security) needs to develop test methods and standards (*e.g.*, how clean is clean, environmental tolerances for effluent, etc.), to compare against current decontamination technologies in responders' scenarios. Testing and standards are critical to increasing responders' capabilities in this area in the near-term, even with significant investments. Some of the testing and evaluation can be accelerated, to shrink the timeline two to three years.

Gap-fillers to address responders' requirements include:

- A modeling and simulation exercise/feasibility analysis focusing on specific scenarios and agents, to evaluate existing decontamination technologies.
- Development of a highly intuitive Graphical User Interface (GUI) for equipment Personal Digital Assistant (PDA) or laptops in vehicles to augment the training for the emergency responder community.
- Establishment of a digital capability that will provide a picture (graphs) regarding action to be taken upon arriving at a chemical/biological incident (*i.e.*, 1-800-CHEMBIO). This system would answer questions right away and prevent unnecessary efforts, delays or lost time (this gap filler is similar to those called out in DIDA.3 (*Classification and Mitigation*)).
- Research for "Effluent Decontamination and Disposal." A program for how to track this by-product is needed. Binding agents could be added to help contain the effluent and prevent secondary contamination on city surfaces or sewers; additionally, other chemical additives could be used to neutralize (anti-bacterial, base for acids, etc.) harmful effects to the environment.
- Distance learning technologies, to convey decontamination procedures and standards, for delivery to "networked learning centers" (*i.e.*, fire houses or National Guard facilities).
- Cross-cutting capabilities from other NTROs (especially Unified Incident Command and Emergency Management Preparedness Planning), such as incident command/mission planning software (*e.g.*, overlays) will help in establishing decontamination site boundaries (zones), associated weather conditions, etc.

R&R.2 – Rapid Decontamination of High Value and Critical Response Equipment. *The ability to identify contaminated equipment, isolate it or move it out of the warm zone, and remove contaminants to a verifiable level of "clean," in order to rapidly return equipment to service in the midst of an emergency.*

Goals:

- Rapid return of equipment to service (<1 hour).
- Two levels of decontamination: for emergency use and reuse, and definitive decontamination.

Current Capabilities:

- Responders felt the current capabilities for this functional capability were identical to that of mass victim decontamination: a marginal capability exists today (irrelevant for high explosive/incendiary).
- Currently, much equipment has to be destroyed because it cannot be decontaminated. This is a significant cost to jurisdictions.

State of the Art:

There are a number of technologies under development. Resource management and tracking technology is available and can be engineered to

accommodate this application. Materials science products under development by Nuclear/ Biological/Chemical (NBC) survivability programs are an example of this possibility. These products include contamination-resistant materials and paint: a Soldier and Biological Chemical Command (SBCCOM) (now Edgewood Chemical and Biological Center (ECBC)) report, *Comparison of Decontamination Technologies for Biological Agents on Selected Commercial Surface Material* (April 2001), evaluates available technologies (mostly research-scale) based upon their ability to reduce the spore contamination on panels of different materials representing office environments. The study also examines chemical agent resistant coatings (paint) which could be used on high-value equipment. These efforts could be applied to emergency response equipment, but the technology is currently too expensive.

Water is still a primary decontamination material, but is usually detrimental to electronics. Technology does exist to protect electronics, and could become part of a "standard" for new equipment going forward. However, the cost to retrofit the embedded base of equipment would be prohibitive.

Other technologies and products are under development by the Defense Department. In applying these technologies, there will be issues related to technology transfer and commercialization. Some efforts are underway to identify strategies for technology transfer out of the military arena and into civilian hands, especially emergency responder, use. It is plausible that the response community will provide new markets for those products and technologies, which might help drive costs downward into the affordability range for local jurisdictions.

Technology Limitations and Barriers:

The technologies needed to raise the level of capability in this area are of moderate technological risk, and will require more research rather than technology transfer.

Technologies in these areas will inherently depend on sensors to automatically track equipment being committed to the contaminated zones. Some organizations manually bar code equipment going into a hazardous area, but that will not work effectively in a WMD event as it will become time-prohibitive, and manual efforts are error-prone.

Contamination-resistant materials and materials science will be expensive, but the option to sacrifice large quantities of high valued equipment is not efficient: equipment should be decontaminated and returned to service for use on the next call.

Cost is a significant challenge for the availability of materials, polymers, etc. Technology transfer and commercialization strategies (*e.g.*, marketplace incentives) are not mature.

Gap Fillers:

This functional capability is reliant on resource management and decontamination technologies. The government needs to develop and evaluate resource management concepts for identifying, finding, indexing, and limiting use of contaminated equipment during crisis, as well as managing the usability and safety of equipment that will be used and kept in the "hot/warm" zones. As technology for resource management becomes available, associated procedures will need to be developed to quickly identify critical equipment needed for specific events. Electronic communications will be paramount under these conditions (see Chapter IV (UIC)).

Methods need to be developed and tested to detect equipment degradation after decontamination technologies have been applied. Decontamination will have some negative effect on the life expectancy of the equipment. Prototypes can be built and studied in materials science labs, but large-scale production of protective polymers for use today will be a manufacturing challenge.

Decontamination technologies can mitigate reliance on resource management and fill gaps in this overall capability. Such gap-fillers include:

- Development of materials science programs for CBRNE survivability/contamination-resistant emergency equipment;
- Research to create a "plastic casing" to encase and seal equipment without degrading functionality;
- Water resistance appliqués/membranes for electronics to enable the use of water as a decontamination agent;
- Research concepts of providing a "multi-layer" system that could be removed and discarded for rapid equipment reuse;
- Research and development in manufacturing science/engineering and equipment design to allow rapid maintenance/replacement of degraded parts;
- Research to provide dosimeter type components/instrumentation to signal when equipment is becoming unsafe.

R&R.3 – Establishment of Perimeters. *The ability to identify, establish, manage, and control (including inter-zone movement and control of flow between) hot, warm and cold zones and security perimeters.*

Goals:

- First units on scene, regardless of discipline (*e.g.*, law enforcement) can recognize hazard and quickly (within minutes) determine and verify hot zone.
- Ability to establish (cordon) and communicate hot zone to arriving units.
- Security perimeter established and secured within minutes by first arriving law enforcement.
- All perimeters modified (expanded or contracted with varying levels of security) as necessary in real-time.

Current Capabilities:

- This capability exists today in the high explosive/incendiary operational environment.
- This capability is marginal for the chemical, radiological, and nuclear environment, and non-existent for the biological operational environment.
- In general, this functional capability depends heavily on detection, identification, and assessment capabilities. (See Chapter III (DIDA).)

State of the Art:

Currently, situational awareness technologies such as cameras in a police cruiser or at intersections can be employed to establish perimeters. By assessing and leveraging the technologies in place from both public and private enterprises (subways, parking lots, automated teller machines, etc.) self-generating perimeter concepts can become a reality.

Modeling technologies also exist which can be used to provide suggested responses such as perimeter sizes. These technologies have existing scenarios built-in, and will automatically monitor the aspects of an event, whether it be a "what-if" simulated event for training purposes, or a real event. The tools use detailed computer algorithms and data processing architecture using specifically tailored expert assistance logic and high-speed data manipulation techniques.

Technology Limitations and Barriers:

This capability element is reliant mainly on technologies from Chapter III (DIDA) for sensors and Chapter IV (UIC) for communications. There are significant challenges in having detection technology (to know if the situation is changing), and communications technology (to know where your people are, and to communicate reliably with them). Real-time detection is needed to decide if the perimeter needs to change due to weather changes, perimeter breaches or unknown parameters that may be uncovered during the event. Plume modeling technology is available but training and sensor placement is required for it to be effective.

Gap Fillers:

- Development of vehicle instrumentation with DIDA technologies that can be integrated with vehicle-mounted geographic information system (GIS) capabilities to "model" a perimeter.
- Development of systems that integrate sensors into perimeter modeling tool-kits, with sensors and communications that are weight-neutral and integrated into standard equipment (*e.g.*, police badges) and linked into GIS, C^2, modeling systems, etc.
- Development of technology suites, advanced systems and concepts so that potential target sites can self-generate perimeters, by inputting data into arriving personnel GIS and modeling systems.
- Use of wireless and internet technology to move pictures/information to responders and back to command posts while still in the assessment stage of the incident.
- Leverage current infrastructure capabilities like the Department of Transportation's (DoT's) camera and monitoring equipment used in metropolitan areas.
- Systems integration of all the above needs to be developed. All of the "piece-parts" are available.

R&R.4 – Functioning in the Absence of Critical Infrastructure and Restoration of Essential Public Services. *The ability to carry out the critical missions of the organization in the absence of facilities and utilities that are normally available, and then decontaminate, reconstruct, and reactivate government and private services, mechanisms, and processes that serve as or support essential public services, including emergency services, food and water, electricity, sanitation, and other functions that directly support immediate human needs.*

Goals:

- Operation for twelve hours in the absence of critical infrastructure.
- Restoration of essential public services (*i.e.*, those needed for assuring the lives and well-being of the public in the vicinity) within three days.

Current Capabilities:

- Capability is available across the spectrum for responders to function in the absence of critical infrastructure for twelve hours.
- Capability is marginal for responders to restore essential public services within three days for all but nuclear operational environments. Capability does not exist to restore public services within three days of a nuclear attack.

State of the Art:

A variety of programs exist within the Federal Emergency Management Agency (FEMA), DoD, and the Nuclear Regulatory Commission (NRC) to provide solutions for functioning in the absence of infrastructure and quickly and temporarily restoring critically needed public services. These programs include long-lived power sources, smart cables for power conversion, quickly erectable communications towers, multi-fuel compatible generators, and alternate power sources. Many regulatory agencies provide for methods and procedures to assist with natural disasters such as forest fires, earthquakes, and floods. These methods and procedures are directly applicable to man-made terrorist events.

Technology Limitations and Barriers:

Cost is a main barrier. Technologies will need to be purchased in "quantity" to be affordable to all. Emerging power sources are still very expensive. Capability is reliant on power sources, such as solar, wind, gasoline, battery, etc. The small manufacturing base in this area does not push the envelope on battery development as demand is low or limited to highly specialized equipment in the DoD. As a consequence, R&D programs for the desired technology is sparse or directed to very specific products or agencies/departments.

Gap Fillers:

- Development of lightweight long-lived power sources (*e.g.*, batteries) and recharge technologies (*e.g.*, photovoltaics).
- Development of alternative micro-power sources.
- Development of power management in electronics design (energy efficiency design).
- Development of multi-fuel engines.
- Systems engineering to integrate national monitoring of critical infrastructure interdependencies into jurisdictions' response capabilities.

R&R.5 – Health and Crisis Response Education. *The ability to develop and disseminate a public education program to help prepare the public psychologically and physically to deal with the effects of the attack, to make them aware of emergency procedures and services in the event of the attack, and to make them understand the necessary requirements they must fulfill or be aware of (e.g., first aid, personal decontamination, hazard avoidance, etc.) in the aftermath of an attack.*

Goals:

- A checklist in each citizen's house, as well as schools and businesses.

Current Capabilities:

This capability exists today for the nuclear environment, but is marginal for the other operational environments.

State of the Art:

There are several programs and public information campaigns that successfully address cross-cultural/language barriers and could be used as models. Examples include: the National Libraries of Medicine Breast Cancer campaign; the U.S. Department of Agriculture's (USDA's) food safety program, and E9-1-1. Other public information programs provide a model for incorporating education with technology: National Weather Service, Amber Alert System, reverse 9-1-1, Emergency Notification Systems and Emergency Broadcast System. The Department of Transportation (DoT) has a broad range of diverse technologies, known collectively as intelligent transportation systems (ITS), which might fulfill many of these needs. ITS is comprised of a number of technologies, including information processing, communications, control, and electronics. There are a number of other federal models to draw upon: for example, following the accident at Three Mile Island in 1979, the Nuclear Regulatory Commission (NRC) reexamined the role of emergency planning for protection of the public in the vicinity of nuclear power plants. The Commission issued regulations requiring that before a plant could be licensed to operate, the NRC must have "reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency." The regulations set sixteen emergency planning standards and define the responsibilities of licensee, and State and local organizations involved in emergency response.

Finally, there are a number of capabilities within the private sector for training and awareness into which terrorism planning is being or can be incorporated. One such example is CorpNet, for business continuity planning education. Another example is the Partnership for Public Warning (PPW), a partnership between the private sector, academia, and government at the municipal, state and federal level. The PPW's mission is to develop a consensus on process, standards and systems that will provide the right information about dangers to life and property to the right people, in the right place, and at the right times, so those in harms way can take timely and appropriate action to save lives, reduce losses and speed recovery – whether from natural disasters, accidents or acts of terrorism.

Technology Limitations and Barriers:

- There are no "technology limitations" in delivering information. However, there are "barriers" to delivery: multi-lingual, multi-cultural, education levels (documentation should not exceed a fifth grade level), and distribution methods to assure information reaches every household.

- Technology is available for notification to the public-at-large (homes, offices), however there is no demand or push by emergency management at the national or state levels. A program of this type would incur large upfront costs. However, this will not happen without a good business case or mandate or both.

Gap Fillers:

- Enhancement of current technologies with notifications systems such as: Community Notifications System (CNS), Carrier Grade Notification System (CGNS), Emergency Notification System (ENS), Remote Surveillance Support System (R3S).
- Create a program based on three factors: awareness, education (dealing with generic problems/situations and generic answers) and training.
- Work within existing projects and organizations (above) in the government, private sector and academia to establish a national awareness program.

R&R.6 – Specialized Search and Rescue Capabilities. *The ability to rapidly locate, assess, and rescue, injured and/or contaminated victims in a CBRNE environment with or without structural collapse.*

Goals:

- Safely locate, disentangle and remove victims quickly and efficiently.

Current Capabilities:

- FEMA's Federal Urban Search and Rescue (USAR) Task Forces represent the highest level of capability today, with listening devices, search cameras, and robots for detection and extraction. Most jurisdictions do not have a Federal Task Force.
- In addition to this uneven national capability, even Federal Task Forces today have a marginal capability to do specialized search and rescue in a contaminated environment, especially in a biological operational environment.
- In a terrorist event, the time it takes for a USAR team to respond (two to four hours) is insufficient to allow for rescue operations. By the fourth hour, it is a recovery operation.
- USAR teams have capability to temporarily stabilize collapsed structures and rubble piles.
- There is limited access to specialized search and rescue training for non-USAR personnel.

State of the Art:

The FEMA USAR task forces currently carry search cameras, acoustical devices, and smart levels (for structural engineering) as standard rescue equipment. However, FEMA Task Forces are not available for response, per policy, unless disaster includes collapse of a reinforced concrete building. All 28 FEMA teams will be upgraded to WMD capable, which will allow them to enter a hot zone for short periods of time. Extended time will be dependent on new PPE and the availability of relief workers and the extent of time required on scene. Various technology components are available for an emergency responder technology platform. However, the effectiveness cannot be determined until requirements are provided. Engineering/integration, standards and operational test and evaluation (OT&E) are critical to overall effectiveness of the needed technology.

Technology Limitations and Barriers:

- Ground penetrating radar (GPR) capability exists for up to ten feet of earth. The ability to look through 30-50 feet of rubble is currently a technological challenge (GPR has been researched extensively with limited success for land mine detection).
- Sensor suite for robotics is a question of requirements, packaging and cost, not engineering. Radar can be made to work with robotic arms, etc. Requirements need to be generated to match the responder mission (weight constraints, power, endurance, standards, etc.).
- Standardized caches of equipment will need to be flexible, one-suit-fits-all.

- Communications challenges are inherent in transmitting out from under rubble, in/out of a building, etc. (This barrier is probably best overcome by ultra wideband communications technology, a recommended Strategic Research Area described in Chapter I.)

- Personal protection technology (see Chapter II (PPE)) advances are needed to improve endurance in a WMD environment. Power source materials are also a challenge for these operations.

- Cost limitations for local jurisdictions apply here, as well.

- The challenges of packaging components at the device level (weight, range, etc.) depend on requirements. This is an area of low technology risk. The various components exist. Technology for packaging and manufacturing require research. With funding this can be achieved within three years. Basic work is already being reviewed by the Communications Electronics Command (CECOM) in support of DHS.

Gap Fillers:

- Upgrade of all USAR Teams to be WMD-capable as soon as possible.

- Standards and test and evaluation (T&E) for ground penetrating radar for application in this functional capability.

- Development of ultra wideband communications capability in an operational package that sends telemetry further up the command chain, beyond the on-scene rescue unit (see Chapter IV (UIC)).

- Standards and T&E for ultra wideband communication technology (see Chapter IV (UIC)).

- Development of requirements for applying the various sensor suites, platforms, robotics, batteries, etc. which already exist.

- Engineering for packaging all the various components into a suite to make a ruggedized capability, followed by operational testing and evaluation.

- Research and development in acoustic detection, improved ground penetrating radar, robotics for gas detection (carbon dioxide (CO_2) detection for victim location), etc.

R&R.7 – Evacuation/In-Place Shelter Management. *The ability to manage public access to relocation destinations, and planning and deployment/location and direction to in-place shelters for those citizens for whom evacuation is not possible or necessary.*

Goals:

- In-place shelters to handle 1000 persons.

- Climate control.

Current Capabilities:

- The capability exists today for the high explosive/incendiary environment. The capability is marginal for all other operational environments.

- Evacuation plans have not been established for most major cities in the U.S., besides those at risk from hurricanes.

State of the Art:

Technology is available to build emergency infrastructure, provide ballistic protection, and place high energy particulate air (HEPA) filters to temporarily cover heating, ventilation and air conditioning (HVAC) systems. Evacuation and sheltering is more of a policy, planning and management issue with complex managerial and psychological impacts. The Red Cross has established shelter in place guidelines. From the DoD side, the Defense Advanced Research Projects Agency (DARPA) has "Force Provider," which provides temporary shelter for mobile population in crisis, and the "Immune Buildings Program," which can provide technologies and solutions for in-place sheltering.

Technology Limitations and Barriers:

- Management of the process is more of a challenge than technology development (*i.e.*, quarantine situations, public access and control, media relations, communication and education, integrating plans with technology suites for evacuation routes, integrating plume modeling, and ability to communicate once the evacuation starts.

There is little technological risk in developing programs to meet these capabilities.

Gap Fillers:

- "Force Provider"-type pre-positioned structures should be stored at regional depots in the U.S. ready for deployment to house evacuated or to isolate and control contaminated population.
- Use of business contingency planning organizations/media to include evacuation/shelter-in-place planning as part of their industries core requirements when developing company/family contingency plans.
- Initiation of a new National Evacuation Program similar to the FEMA Fallout Shelter Program.

R&R.8 – Residual Hazard Assessment and Mitigation. *The ability to identify, assess the presence and danger of, and mitigate lingering presence and effects of threat agents, secure still-dangerous areas, and manage waste and effluent from contaminated areas.*

Goals:

- No secondary contamination.

Current Capabilities:

This capability exists today across the spectrum of operational environments. However, the capability is dependent upon emergency management preparation and planning functions. (See Chapter VI (EMPP).)

State of the Art:

Most major jurisdictions have in-place programs and plans to comply with regulations prescribing this functional capability, promulgated by, *e.g.*, FEMA, EPA, DoT, etc.

Technology Limitations and Barriers:

The ability to address and mitigate any "residual hazard" is highly dependent on the community's capabilities and availability of resources. It is probable that metropolitan areas will have local control and response capabilities which will quickly move to apply EPA guidelines, address any particulate contamination and take steps to alleviate the effects.

Gap Fillers:

Apply decontamination technologies that are available or will be developed, *e.g.*, in R&R.1 (*Mass Victim Decontamination*), R&R.2 (*Rapid Decontamination of High-Value and Critical Response Equipment*), etc.

R&R.9 – Mass Fatality Management. *The ability to contain, decontaminate, remove, and track fatalities.*

Goals:

- Collection, preservation of the body (suitable for open casket).
- Positive identification of the body.
- Maintenance of evidence.
- Preservation of personal effects.
- Notification of the next of kin.

Current Capabilities:

- The capability exists today for hazardous materials (HAZMAT) units to perform this function, with the exception of a biological operational environment, for which no capability exists today. However, HAZMAT units will not turn to this mission until they are finished dealing with live victims.

- Coroners do not have this capability for any operational environment except high explosive/incendiary.

State of the Art:

There are procedures in place to address fatalities caused by a terrorist attack using chemical, nuclear and high explosive devices. The National Medical Response Plan created a Disaster Mortuary Operational Response Team (DMORT) consisting of fifty personnel in training to respond to a "mass fatality incident." However, under the best circumstances the DMORT team can decontaminate up to fifty bodies in a twenty-four hour period. Biological and radiological (dirty bomb) decontamination does not have sufficient documentation to determine how decontamination will be handled for external and internal cleansing of the remains. These contaminants raise serious concerns and questions as to what the disposition of the remains will be once a decontamination process is complete. While the goal of the DMORT team is to preserve the body, preferably for open casket viewing, there may be an unwillingness on behalf of the local mortuaries to receive decontaminated remains without an agreed measurement that defines what "clean" is.

Current technology for "food irradiation" has been partially successful. This technology (*e.g.*, Sure-Beam) was applied in decontamination efforts of post office facilities after the October 2001 anthrax attacks. The technology could be applied to biological decontamination.

Chemical/biological body bags heat-sealed, with gaseous decontamination, is a concept under development. However, there are issues with transporting contaminated remains to a decontamination site.

Technology Limitations and Barriers:

- Political, religious and cultural considerations drive the technology requirements.
- Biological decontamination of bodies must be internal as well as external.
- If decontamination is not an option, bodies might have to be cremated. However, sufficient cremation capabilities do not exist in the U.S. for an incident involving mass fatality.
- Food irradiation and gaseous decontamination technologies are promising, but are also very large and not easily mobile.
- Irradiation technologies pose specific problems in radiation management, transportation of bodies, metrics for cleansing bodies internally, facilities vs. numbers of dead to be decontaminated, etc.

Gap Fillers:

- Adaption of gaseous decontamination and food irradiation technologies to this capability.
- Mobilization and miniaturization of irradiation and gaseous decontamination technology.

R&R.10 – Traffic Management. *The ability to manage traffic in evacuation and around incident site, to include knowledge of traffic flows, alternative routes, relocation routes and destinations, and accidents/traffic blockages.*

Goals:

- Real-time traffic re-routing.
- Knowledge of "flow" (*i.e.*, number of cars, their destinations, etc.).
- Ability to handle evacuation of >100,000 vehicles.

Current Capabilities:

A marginal capability exists today, across all operational environments.

State of the Art:

Traffic management capabilities exist today and are employed in most major cities. Nevertheless, more sophisticated products could be developed that would allow for dynamic rerouting while maintaining the integrity of the "final destinations" selected to house evacuees. The U.S. Army has technologies and algorithms for

situational awareness, traffic routing and re-routing, alternate routing and timing, knowledge of blockage. Simulation programs can be created from these technologies to provide "sensible evacuation routes and policy/procedures" depending on strategic decisions at the time of the particular incident. Each urban area will differ on a day-by-day basis depending on road maintenance (closures or bottlenecks), construction etc. It will be important to have a collaborative tool to practice traffic management in a crisis mode and identify known shortcoming and areas for improvement.

Technology Limitations and Barriers:

- A major metropolitan area will never have enough personnel and assets to deal real-time with a mass evacuation traffic crisis.
- This functional capability is reliant on perimeter establishment and security technologies, and interoperable communications.

Gap Fillers:

- Systems integration: GIS visualization technology, fed by rapidly reconfigurable sensor suites, integrated with other existing products for traffic control, perimeter establishment and control, etc.
- Pre-planning with communities that will be receiving the evacuees (see R&R.7 (*Evacuation In-Place Shelter Management*).)
- Use of message boards that can be towed into place or messages displayed on electronic signage if applicable.
- A designated radio broadcast channel for emergency information in each urban area.

R&R.11 – Incident Action Planning. *The ability to implement a process that starts with pre-event planning, and then assessment, identification of goals and objectives, strategy for dealing with situation, assignment of tasks, and follow-up.*

Goals:

- Part of a unified incident command process.
- Written, formal documentation (continually updated) by the start of the "second operational period" (in responders' terms).
- Plan that covers all agencies/activities relevant to the incident, to include functional annexes for each agency that participates in unified incident command.
- Includes a safety plan and a medical plan and may include other event specific plans.
- Disseminated in all operational periods.
- Integrates GIS, expert systems, sensors and processing systems (tied into detection, etc.) and shared databases/information systems on readiness and availability of response assets, integrated as a comprehensive web based system to determine which plans and capabilities are appropriate for the incident scenario.
- Includes post-incident analysis and corrective action program.

Current Capabilities:

There exists today a marginal capability for this function. Larger jurisdictions with a dedicated Office of Emergency Management have a stronger capability in this functional area.

State of the Art:

Today, incident planning technologies exist but will require integration and standardization into such structures as the National Incident Management System (NIMS), etc. It is critical to be able to provide on-the-fly managing of assets and people along with knowledge of terrain and operational area and have the flexibility of re-tailoring and distributing scenarios and plans. The DoD has a great deal of experience in this area, with programs such as DARPA's Command Post of the Future, and the U.S. Navy Space and Naval Warfare Systems Command's (SPAWAR)

programs to integrate situational awareness systems into command post systems. Many planning tools have come out of these efforts, which could be leveraged to the emergency responder community.

Technology Limitations and Barriers:

- This problem is process-intensive, and not limited by technology barriers.
- Planning is reliant on all-source situational understanding and unified incident command. (See Chapters IV (UIC) and XI (ASU).)
- Common standards are required for interoperability.
- Training issues are inherent, including strain on personnel, readiness, cost and time needed for training, etc. Technology must be highly intuitive and flexible (multimedia and flexible in time).

Gap Fillers:

- Affordable and highly intuitive common suite of tools (GIS, satellite phones, video teleconference (VTC) capability, interoperable communications link, software, etc.) integrated into the NIMS, etc.
- Training technology to facilitate deployment of this capability.

R&R.12 – Public Relations and Media Management. *The ability to accommodate the logistics requirements of the on-scene media encampment, to provide the media necessary information critical to informing the public of the threat and associated emergency directions (e.g., evacuation, danger areas), and to manage the safety of the media (their physical safety).*

Goals:

- Established process for using media resources for enhancing public safety (site cameras, helicopters, satellite connectivity).
- Use of media assets to help emergency operations.
- Control of airspace.
- Dissemination of accurate information.
- One unified voice, in a qualified public information officer that the represents the unified command structure.

Current Capabilities:

This capability exists today.

State of the Art:

Media firms and government agencies have long established crisis communications plans that include designations for media encampments, logistics for power, water, etc. However, media coverage of disasters has increased public expectations for government response.

Technology Limitations and Barriers:

There are no significant technology limitations for providing this functional capability. Difficulties arise only in policy or planning issues, such as education of responders and government officials in the methods and procedures necessary for dealing with a terrorist event, and the control of sensitive information during ongoing crises or law enforcement investigations.

Gap Fillers:

Media plan for terrorist events, refined to take into account lessons learned from recent history (*e.g.*, 9/11, Iraqi campaign, etc.).

Response and Recovery Response Technology Objectives (R&Rrto)

R&Rrto.1 – Contaminated Victim Knowledge Base

Objectives:

Develop a tool for emergency responders to use in determining how to respond to a mass chemical, biological or radiation contamination event. Using data provided by available sensors and information stored before the event, the tool will provide responders with the best course of action to begin the decontamination of large numbers of victims. The tool will facilitate rapid identification of the presence and type of contaminant, communicate results to a knowledge base, and

provide responder with recommended course of action. The tool should include a highly intuitive Graphical User Interface (GUI) and be useable on a Personal Digital Assistant (PDA) or a laptop in a vehicle. It should have the capability to provide graphics regarding action to be taken upon arriving at a chemical/biological incident. See also DIDA.3 (*Classification and Mitigation*) and DIDA.8 (*Pre-Triage/Differentiation Among Levels of Exposure*) for application to other needs.

Payoffs:

This will help emergency responders effectively identify, isolate and prepare to decontaminate victims. It will help to save lives and prevent spread of contamination.

Challenges:

The development of such a tool is considered low risk, however its utility will depend on the real-time data about the incident and the nature of the decontamination it uses. Availability of real-time data is dependent upon the development of new and improved sensors, which are addressed in Chapter III (DIDA).

Milestones/Metrics:

FY2004: Benchmark similar systems for developing course of action recommendations. Develop architectural design for the tool, collect and integrate existing information.

FY2005: Develop a prototype of the tool and begin emergency responder testing. Begin commercialization effort to aid in transition to responders.

FY2006-2008: Integrate and deploy systems for emergency responders while continuing to integrate new products and methodologies into the system. Complete commercialization effort.

R&Rrto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Develop Integrated Technology Suite (Toolkit) Pilot	$5	$5	$5	$5	$5	**$25**

R&Rrto.2 – Protective Coatings for Critical Equipment

Objectives:

Develop materials and appliqués that will resist contamination or facilitate rapid decontamination without degrading sensitive equipment such as electronics, such that critical equipment can be rapidly returned to service within the contaminated zones in less than one hour.

Payoffs:

Enables rapid return to service of critical equipment that is too expensive or important to be discarded, without causing secondary or continuing contamination to personnel or environment.

Challenges:

Much of the equipment needed by emergency responders is electronic in nature and may not be able to be cleaned using convention cleaning procedures (*e.g.*, water) or returned to service within one hour. Protective casings impair functionality or usability of equipment. Materials science faces technological challenges. (See Chapter I for a discussion of materials science as a Strategic Research Area.)

Milestones/Metrics:

FY2004: Identify and evaluate potential enabling technologies.

FY2005: Begin research or applied technology effort on new materials and coatings as indicated by evaluation process in the previous year. Develop metrics for evaluating "clean."

FY2006-2007: Develop and test alternative protective coating concepts for several common, high-value pieces of responder equipment.

FY2008: Develop prototype protection packages. Test packages in operational environment. Begin commercialization efforts to transition technology to use.

R&Rrto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Protective Coatings	$15	$22	$25	$18	$10	**$90**

R&Rrto.3 – Ground Penetrating Radar for Specialized Search and Rescue

Objectives:

Develop and demonstrate an affordable ground penetrating radar system to assist search and rescue operations, in order to rapidly locate, assess, and rescue, injured and/or contaminated victims in a CBRNE environment with or without structural collapse, including location of live victims buried in tunnels or beneath reinforced concrete up to fifty feet.

Payoffs:

Rapid response and greater chances of recovery of injured victims.

Challenges:

Penetrating reinforced concrete or dense rubble. Penetrating radar capability exists for up to ten feet. The ability to look through 30-50 feet of rubble is currently a technological challenge.

Milestones/Metrics:

FY2004: Define requirements for applying ground penetrating radar for urban search and rescue operations in a CBRNE environment. Identify existing programs in DoD and industry and create a development consortium to accelerate the product development.

FY2005/2006: Develop and engineer a search and rescue Ground Penetrating Radar (GPR) prototype. Develop a commercialization plan using consortium members.

FY2007: Begin field testing GPR prototype. Demonstrate capability in a large-scale urban search and rescue exercise.

FY2008: Complete commercialization of GPR and transition to use by emergency responders.

R&Rrto.3 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Ground Penetrating Radar	$5	$10	$15	$20	$5	**$55**

R&Rrto.4 – Irradiation and Gaseous Decontamination for Mass Fatalities

Objective:

Adapt irradiation and gaseous decontamination technologies and methods (*e.g.*, food irradiation and concepts used on postal facilities after October 2001 anthrax attacks, etc.), for mobile use in a mass fatality incident.

Payoffs:

Safe handling, tracking, and delivery to family, of decontaminated remains, without degrading the decedent's suitability for open casket funeral.

Challenges:

Radiological containment safeguards; mobility of large equipment for irradiation/gaseous decontamination and fatality processing; verification of biological decontamination, especially inside corpses.

Milestones/Metrics:

FY2004: Develop requirement for applying irradiation and gaseous decontamination technologies to this functional capability, to include safety/surety (*e.g.*, radiological surety) systems and concepts.

FY2005: Identify and evaluate potential enabling technologies and procedures.

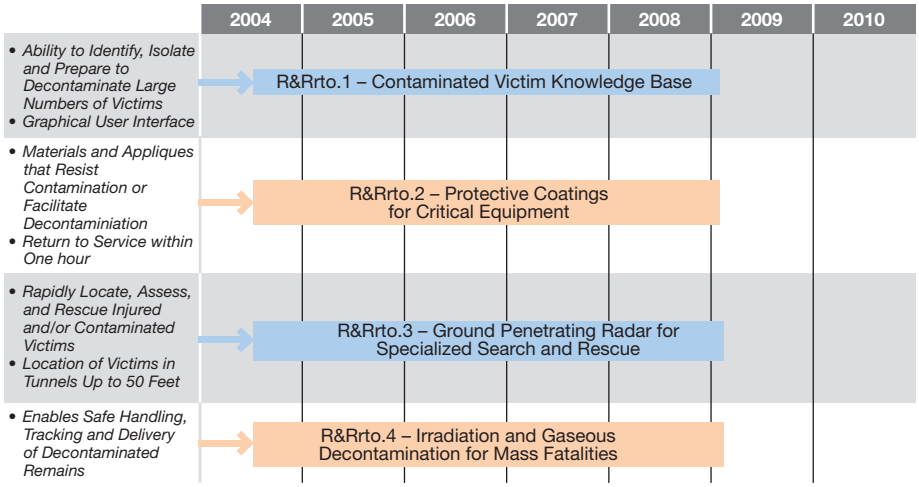
FY2006: Engineer solution based on technologies found. This will likely require making the technology small enough to serve the function's logistical needs.

FY2007: Continue engineering development and begin testing equipment and concepts of operations. Develop methods and procedures; training programs.

FY2008: Demonstrate capability in a mass fatality exercise. Transition to use.

R&Rrto.4 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Mass Fatality Decontamination	$3	$4	$16.5	$15.7	$15.7	**$54.9**



Response and Recovery Technology Roadmap

Chapter VI

Emergency Management Preparation and Planning (EMPP)

Chapter Chair: Brett Kriger
Chapter Coordinator: Dr. Maria Powell

Definition

Emergency Management Preparation and Planning (EMPP) is the capability to perform vulnerability analysis of high-risk facilities and locations, plan responses to various terrorist scenarios, perform low-cost high impact training for terrorist incident response, and coordinate among local authorities before a terrorist attack. This capability objective focuses on preparation and planning across all phases of comprehensive emergency/disaster management.

Operational Environments

The operational environments for this NTRO are: chemical, biological, radiological, nuclear, and high explosive/incendiary. The type of event responders must address dictates the needs of incident commanders, and thus the demands on the EMPP support structure to manage the preparedness, support coordination, and resources needed by incident commanders.

However, from the perspective of the emergency manager, the type of event or threat scenario is not the critical factor in developing an effective and coordinated response and recovery system. In most jurisdictions, the emergency management and EOC function are required to take a multi-hazard/risk perspective. Plans call for the EOC to deal with the complexity of cascading events and constant variations in response priorities.

Some objectives will describe needs for a workspace that supports the functional staff during their various emergency support tasks. That workspace has some variations in its nomenclature but is generically referred to as an Emergency Operations Center (EOC). The EOC has a role in all phases of emergency management:

- In the preparation phase, the EOC is functional and prepared for any contingency. It is used for orientations, training, and exercising.
- In the emergency response phase, the EOC along with supporting department operations centers, serves as the central point for agency or jurisdiction coordination and overall management of the emergency.
- In the post emergency or recovery phase, the EOC can be used to house supporting organizations and direct the recovery operation.

It is important to note that EOCs do not directly manage or "command" incidents. "Command" implies setting incident objectives, determining strategy and tactics, and assigning and supervising tactical resources. This is the role of the on-scene incident commanders using the component elements of the Incident Command System (ICS). The EOC is part of the support structure for the ICS and its commander, but the EOC does not command, it coordinates and supports. In a complex incident involving multiple agencies and organizations there may be a more elaborate coordinating structure within the EOC that is usually referred to as Unified Incident Command or the Incident Management System.

Responders emphasized that emergency response is initially dependent on local resources and capabilities. The system at the local level must be adequate to support the initial response and then smoothly expand to encompass regional, state, and/or national multi-agency coordination. This ability to expand rapidly and integrate resources to supplement the original local response involves:

- Establishing priorities for response.
- Allocating critical resources.
- Developing strategies for coordinating multi-agency and inter-agency response problems.
- Sharing information.
- Facilitating communications.

Needed Functional Capabilities and Priorities

Responders emphasize that the coordination and support for all stages and levels of the threat spectrum must be addressed. However, emergency management is generally focused on preparedness strategies that provide for impact assessment, resource prioritization, and consequence management. These strategies originate with decision-makers who function collaboratively in EOCs. The traditional capabilities of EOCs are based on the readiness and effectiveness of emergency response services to respond jointly to a significant event that is beyond the capability of any one agency or organization.

Response to a major terrorist event places greater demands on the management system than other large-scale incidents. The initial response would be quickly supported by multiple agencies from all levels requiring a rapid assemblage of diverse capabilities, some from distant areas that have little operational familiarity with the others. This would occur in the midst of confounding uncertainties, limited resources, conflicting priorities and potentially tragic misdirection. Many responders, lacking clear guidance, would simply react to apparent immediate needs.

The complexity of coordinating and prioritizing the resources of multiple agencies requires the multilateral sharing of authority to ensure the most rapid and effective response possible. A single manager cannot be directly responsible for all of the efforts needed to minimize this elapsed time. A manager has to have plans, data, and communications to competently work with others as necessary, and to support emergency responders and incident commanders in efficient response.

In a major area-wide incident, there may be multiple incidents of various types within a single jurisdiction. Some incidents may be single-discipline (*e.g.*, fire service) incidents; others may be multi-disciplinary incidents operating under a unified command. The jurisdiction's EOC may be activated to coordinate the overall response, while the Incident Command System is used by field responders. Incident commanders may coordinate their actions through department operations centers which are represented in the EOC. There may also be direct coordination and communications occurring between incident commanders and the EOC. The complexities and difficulties of sharing data and information that is critical to an effective, safe, and timely coordinated response is at the core of this NTRO.

The enabling technologies for these capabilities are already available, in many cases, or in stages of advanced development. Still the capabilities are not generally in place at the local level. In some cases the obstacle is not availability but the complexity of the software, maintaining competence to operate it, availability of data sets, and costs in time and dollars for procurement training, and sustainment. The needed functional capabilities are presented below in order of priority, the first being the highest based on responders' input in workshops and field interviews conducted during the earlier phases of this effort.

- Risk Awareness and Assessment
- Mission Rehearsal, Simulation, Embedded Training and Distance Education

- High-Value Target Identification and Monitoring
- Alternate/Mobile Hospital Contingencies
- Course of Action Development
- Establish Emergency Operations Center
- Facilities/Infrastructure Hardening

The responders rated *Risk Awareness and Assessment* (EMPP.1) as the highest priority within EMPP. Risk awareness is the most important requirement of planning response to a terrorist attack. The next four were rated near each other in priority: *Mission Rehearsal, Simulation, Embedded Training and Distance Education* (EMPP.2); *High-Value Target Identification and Monitoring* (EMPP.3); *Alternate/Mobile Hospital Contingencies* (EMPP.4); and *Course of Action Development* (EMPP.5).

The next highest priority was *Establish Emergency Operations Center* (EMPP.6). The responders thought that, even though this area can use improvement, they are already doing this function in most geographical areas. Finally, *Facilities and Infrastructure Hardening* (EMPP.7) was rated lowest priority because it is not a central function of emergency management.

Overall State of Technology for Emergency Management Preparation and Planning

The matrix below shows a pattern of few technological challenges in meeting the needs of Emergency Management Preparation and Planning. The key challenges will be in the highest priority *Risk Awareness and Assessment* (EMPP.1), but these challenges should not be technologically significant. Technology is available, at least marginally, in the near-term for application in all but a handful of specific areas, even for those areas where capability is marginal (*e.g.*, the highest priority *Risk Awareness and Assessment*) or non-existent (*e.g.*, the third-highest priority *High-Value Target Identification and Monitoring* (EMPP.3)). These technologies can be developed and integrated with little technological risk. This emphasizes the point that capabilities in this response objective can be increased today, through systems integration or even commercial-off-the-shelf (COTS) technologies, as well as from non-technology solutions such as changes in organization, doctrine, and training, and through the development and adoption of standards.

Emergency Management Preparation and Planning

Functional Capabilities	Operational Environments: Chemical	Biological	Radiological	Nuclear	High Explosive/ Incendiary
1. Risk Awareness and Assessment					
2. Mission Rehearsal, Simulation, Imbedded Training and Distance Education					
3. High Value Target Identification and Monitoring					
4. Alternate/Mobile Hospital Contingencies					
5. Course of Action Development					
6. Establish Emergency Operations Center					
7. Facilities/Infrastructure Hardening					

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

EMPP.1 – Risk Awareness and Assessment. *The ability to provide analysis and assessments of threat, vulnerability and criticality of events, venues, and systems (including key assets and infrastructure).*

The first step in emergency management preparation and planning is the understanding of the risks and an assessment of how to address them. The ability to support this process technically

with automated decision aides and other information technology will increase the effectiveness of the analysis and therefore the plans that are derived.

Goals:

- Ability to collect and integrate data on multiple sites.
- Ability to sort and prioritize.
- Identification of potential cascading effects.
- Data sets that employ nationally mandated standards.
- Management of data in secure format.
- Data sharing across jurisdictions, departments (digital format).
- Integration of national information and past experience.

Current Capabilities:

Most technologies needed by this functional capability are available today, irrespective of cost. The consensus is that initial cost is not necessarily the salient issue – lack of integration and usability are the main roadblocks. If integration and usability are taken as the main factor in defining availability, then the capabilities are generally seen as unavailable.

Responders have to quickly assess the situation surrounding an incident that put lives and property at risk. Their knowledge, training, and experience provide the primary basis for the initial actions they take. In addition, responders understand that there are software tools that may help with the risk assessment of key facilities and infrastructure and models that predict impacts; however, there is currently little evidence of widespread use. Much of the software is complex and time-consuming to operate competently and comprehensive data sets needed to make model results useful are not always available.

Even where the technologies (and supporting data sets) are employed, the decision support outputs are incomplete and require additional analysis. There is common agreement that the technologies are potentially available but there is confusion on whose job it is to operate the software, run the models, and conduct the analysis. Most of the software tools typically available to most responders offer only incomplete pieces of the required analysis, and the various systems are not integrated into a comprehensive useable tool.

State of the Art:

There are a number of COTS products that combine agent dispersal and plume modeling (particularly chemical, nuclear, radiological, high explosive, or natural disasters), GIS systems, and database-linked decision support software: many of these products are based on experience with natural disasters. Most of the advanced programs in this area are under active development by the Departments of Defense (*e.g.*, the National Geospatial-Intelligence Agency (NGA) and the Defense Threat Reduction Agency (DTRA)) or the Department of Homeland Security (especially FEMA). Many of these modeling or decision support products are mature enough to have been implemented in various local, state, and federal emergency management organizations.

Technology Limitations and Barriers:

There are no specific technological limitations to achieving these goals. There are some limitations in the area of storage and display capabilities in individual response vehicles, and even greater limitations in the speed of delivery via wireless means in a networked or Web-enabled mode. However, the technologies needed to overcome those restrictions are beyond the scope of this functional element.

Although there are no specific technological limitations or restrictions on data sharing, the issue of interoperable equipment and software has been a concern for many public safety officials because there is not a focused, clearly delineated set of Internet standards for incident management. Improved interoperability and speed of data exchange could be gained with standardization in the Expanded eXtensible Markup

Language/eXtensible Markup Language (EXML/XML) Web programming language.

Gap Fillers:

The next step should be to ensure that the software already utilized is configured such that the needed features have output that is transportable to other EOC software programs.

EMPP.2 – Mission Rehearsal, Simulation, Embedded Training and Distance Education.

The ability to conduct realistic, high-quality training programs and exercises that comply with national training standards (i.e., to meet continuing education requirements).

Mission rehearsal and simulation is generally considered to be a specialized method of delivering training involving realistic practice to accomplish a specific operation or task. There are many commercial systems for accomplishing that activity and the military departments have developed very elaborate methods and systems. Some of the most sophisticated are those employed for training in aircraft and space vehicles.

Embedded training is event- or threat-specific training that could be concurrent with, and thus accompany, other all-hazards training. Examples include chemical terrorism response training that could be combined with "ordinary" HAZMAT training. This would incorporate (*i.e.*, embed) new requirements for specialized skills and knowledge into existing required initial and recurring training. Responders' time is already at a premium for training: most jurisdictions can barely afford the drain on readiness from time away and overtime costs for personnel to keep current with normal-duty training requirements, notwithstanding additional training requirements for terrorism response. Embedded training programs and technologies can create efficiencies in meeting training requirements that save jurisdictions time and money while increasing preparedness for terrorism alongside all-hazards training.

The subject of *distance education* covers a very broad range of training methods that range from posted printed materials (*e.g.*, correspondence schools) to completely Web-based programs. In many cases, the delivery method varies but the same training and course materials may be accomplished either way. The concern about distance learning systems is to ensure the supporting equipment requirements are compatible with what is available to responders in their operating environment (*i.e.*, firehouse, squad room, etc.).

E-learning, Web-based learning, online learning, and distance learning are widely used as interchangeable terms. However, these terms have subtle, but distinguishable differences. Useful definitions for these distance learning systems are:

- E-*learning* – generally covers activities involving computers and interactive networks simultaneously. The computer is not necessarily the central element of the activity nor does it provide learning content. However, the computer and the network are key factors in the learning activity.
- *Web-based learning* – generally covers learning materials delivered in a Web browser, including when the materials are packaged on CD-ROM or other media.
- *Online learning* – associated with content readily accessible on a computer with content accessed on the Web or the Internet, or installed via media (*i.e.*, CD-ROM) on the computer's hard disk.
- *Distance learning* – includes any interaction at a distance between instructor and students, but provides for interaction between instructor and student. Simply posting or broadcasting learning materials is not distance learning. Instructors must be involved in receiving feedback and evaluating level of skill/knowledge mastery.

Distance learning has traditionally referred to televised broadcasts and correspondence courses, and still includes those delivery systems. However, responders were more concerned with reducing the overall training load by ensuring that the requirements for accomplishing levels of knowledge and certifications were carefully crafted and met national standards (few are currently established). The delivery method was not

considered to be particularly important – only that it be effective and efficient.

Beyond HAZMAT response, there are currently no national minimum requirements that cover terrorism training. The Occupational Safety and Health Administration (OSHA) and the National Fire Protection Agency (NFPA) provide for some standards. True national training and credentialing standards would provide for smoother interoperability for multi-agency, multi-level response operations.

Goals:

Training programs and distance education should be:

- Embedded in current systems when possible.
- Embedded in current duties when possible (concurrent training).
- Tailored to different scenarios and localities.
- Supportive of mission essential tasks.
- Re-configurable.
- Interactive at various levels from responder to command to higher authorities.

Training Programs should:

- Be mandatory (100% of personnel within a given timeframe; retraining at given intervals).
- Include testing and assessment.
- Include capture/sharing/implementation of lessons learned.
- Assess particular skills or subsets within training modules, so that trainees do not have to repeat entire modules to learn a narrow subset of skills.

Responders also indicated that training managers and distance learning developers should pursue additional goals as existing emergency response education and training gradually transitions from traditional linear classroom instruction to more interactive, asynchronous, delivery strategies. These goals include:

- Selection of delivery methods and technologies should follow a careful needs analysis that has been validated by responders.
- Availability to as many of the potential extended response teams as possible to include state and local emergency responders, government officials, National Guard units, FEMA, FBI and the Department of Defense. (Participants sharing training are more likely to appreciate each other's roles and develop relationships that will help coordinate efforts.)
- Employment of scenario-based simulation exercises that place response teams in real-life situations through realistic virtual interaction.
- Ability to replay and evaluate the actions taken and decisions made by trainees, so that they can critique their overall performance and set goals for improvement.
- Provisions for sustaining and refresher training are essential regardless of the technology employed.
- Simulations that test critical decision-making skills during all types of CBRNE crisis scenarios, including the more probable scenarios of accidents and natural disasters.

Current Capabilities:

The responders believe that the capabilities to do all the things above are available, especially in the military. However, standards development, minimum skills/knowledge determination, and coordinated funding are required to tailor the technology to emergency responder operational requirements.

Achieving the goals primarily involves changing how responders train, not providing delivery technologies. There is no national standard for training processes, nor is there a central repository for training and exercise coordination. This has created confusion among training methods,

variance in results, and duplicative training efforts.

State of the Art:

Technology to accomplish delivery of automated distance learning is advancing more rapidly than the ability to employ it effectively. The Web has rapidly evolved from a text-only medium to a multimedia communication system with new and varied opportunities for learning at anytime and in any place. The technological revolution enables the teaching-learning process to meet the needs of any responder. More and more training is being made available online but the acceptance of that delivery mode has not been universal. Given the ever-expanding range of possibilities presented by new technologies, training developers must identify processes that work. Educational needs should drive the technology rather than vice versa. Models developed to guide this process often fail to address the specific needs of the adult learner. Standards and guidelines need to align with specific learner needs and program goals.

There are many commercial and military systems and tools available that permit response simulation and rehearsal. These are computer-controlled training systems that simulate specific real-time emergency environments. They effectively allow trainers and incident commanders to evaluate and re-evaluate their management strategies based on dynamic scenarios, including the likely behavior of responders, victims, other people on the scene, vehicles, fires, explosions, chemicals, weather and other environmental factors. The simulator response training and evaluation for virtually any type of emergency should allow for review and repeat for different strategies, procedures, and events. The system also allows users to test and measure the aptitude of emergency responders, allowing them to identify problems and correct them before making a fatal mistake in the field. System costs vary by simulation complexity and range from tens of thousands of dollars to many millions.

Technology Limitations and Barriers:

The adequacy of available bandwidth and installed user equipment was discussed as a technical constraint to widespread implementation. In most of the country (outside the larger metropolitan areas), equipment is rarely state-of-the-art and Internet connectivity (if available) is likely to be via dial-up modem. Many volunteer fire departments don't have computers – legacy-capable or otherwise.

Gap Fillers:

- Improve output of compression using software only (*i.e.*, without the need for high-tech systems or hardware).
- Smart card/chip that contains an "electronic transcript" securely verifying ID, levels and currency of training/certification for outside agency responders that are integrated with local ICS.
- Grant-funded equipment upgrades to ensure adequate multimedia equipment and tools are available for local academies/jurisdictions.
- Use of open source user-friendly tool sets to facilitate customization of training packages by local or regional training managers/academies.

EMPP.3 – High-Value Target Identification and Monitoring. *The ability to monitor high-value targets by retaining their identification, utilizing appropriate monitoring techniques that communicate status whenever needed, and addressing threats as they become manifest and evolve with respect to high-value targets.*

There is no single approach to critical infrastructure protection for every community. Each must address its security concerns to reflect unique aspects of consequences, threats, and vulnerabilities in terms of credible threat, tolerance for risk and ability to mitigate consequences. Leaders and planners must identify the vulnerabilities of numerous assets, and then categorize and rank the risk profiles of the facilities and assets they

identify as critical. The results of that localized analysis are the only basis upon which an effective and credible monitoring and response system could be implemented.

Goals:

Responders described system requirements and needs that are very similar to those of physical protective systems for very high-value targets such as chemical and nuclear weapons storage areas, sensitive military sites, missile sites, and strategic command and control centers:

- 24 × 7 × 365 real-time capability.
- Ability to fuse information from multiple sensors (community infrastructure protection would require integration of tens of thousands of sensors).
- Integration at various echelons (multi-agency, multi-level, and transnational).
- Scalable and on-demand.
- Inclusion of decision aids (such as expert systems for pattern recognition, etc.).
- Secure management of data.
- Validation capability.

Current Capabilities:

Technologies that support these requirements can integrate, sort, and respond to sensors and programmed patterns, but patterns and alarm-level parameters are subject to user interpretation and response determination. These technologies can meet the needed goals, but are contingent on the programming of software for monitoring systems to interpret patterns that users establish. The technologies to install sensors and monitoring systems are available and very capable.

The implementation of these technologies as a consistent capability is very limited within the responder community. Responders and technologists discussed existing technologies that are available but determined that it would be complex and expensive for most jurisdictions to deploy them. Even if the expense for support hardware and infrastructure is provided, the issues of training, pattern awareness programming, and user interface for response will impede effective implementation.

Most localities maintain a list of key assets or likely targets that is updated yearly but these targets have been identified based on traditional risks and threats, such as susceptibility to fire hazards. The sites and facilities that are likely to be attractive terrorist targets may require different examination. The current target lists are initiated and maintained by a building walk-through, and the results are rarely captured in a database or digital format. Current systems are not configured to allow monitoring of targets in real-time from a centralized command center.

State of the Art:

There are no existing programs that are technologically enabled or specialized to auto-generate this information or produce databases that will support visualization. Existing GIS and consequence assessment programs will recognize databases that have been populated with this data but there are no existing technologies that will permit auto- or self-population.

There are extensive existing security systems and sensors which can be employed in conjunction with alarm/switcher/multiplexer interfaces to computer displays to provide a degree of capability to support the stated goals. Sensor technologies include:

- Perimeter monitoring of systems (*i.e.*, traffic cameras/closed circuit television (CCTV)).
- Physical protection systems (security and alarm technologies).
- Satellite imagery.
- GIS/database technology.
- Multi-function unattended ground sensors.
- Seismic sensors for pattern recognition.

Technology Limitations and Barriers:

There are generally no technology limitations or barriers to achieving the stated goals. Monitoring and sensor technology (except for biological sensors that are discussed elsewhere in this report) are very mature and are in widespread use to accomplish the described goals (*i.e.*, nuclear power plants, nuclear weapons storage areas, highly classified military security areas). However, the sensors only report status. The interpretation and decision making must be programmed into automated Supervisory Control and Data Acquisition (SCADA) systems, Programmed Logic Controllers (PLC), alarm switcher/multiplexer systems, or left to the interpretation of human operators.

Gap Fillers:

The goals described above are procedural and operational but could be enhanced by use of available technologies. There are no gap fillers needed for this functional capability beyond those initiatives described in other NTROs (see especially Chapter III (DIDA) for sensor and detection technologies).

EMPP.4 – Alternate/Mobile Hospital Contingencies.

The ability to identify and provide alternate and surge medical locations during pre-event planning.

This capability is needed during any large-scale or catastrophic event whether it is caused by a technological accident, natural disaster, or CBRNE attack. To achieve efficiency, the medical care system is carefully balanced between anticipated need, and in-place capacity. A sudden surge in victims would quickly overwhelm the medical capabilities of nearly any locality. The incident management system would need to designate appropriate alternate and surge medical locations. Hospitals do not generally plan (nor do they have the sole responsibility to plan) for these surge requirements and they do not traditionally have a system for reporting bed-space or staff capacities in real-time.

Goals:

This capability should provide data necessary to a common operational picture for medical needs management, before the overwhelming needs cause a system overload. For example, the urgent care centers should set up an information clearinghouse to continuously match casualty demand with bed supply. Each network would provide information links to its corresponding networks. The hospitals would provide capacity information to the transport network; the on-scene casualty stabilization and triage network would provide casualty information (numbers, types and locations) to the transport network; and the transport network could generate its own transport missions based on need and resource availability.

Major incident or mass casualty response requires rapid communication of the status of emergency medical resources between field units, hospitals, dispatch centers and many other organizations involved in the response. Such information traditionally includes information on the incident or threat, emergency department capacities, bed availability, specific treatment protocols, the status of pharmaceutical stocks, availability of response personnel, equipment and teams, and status of other medical resources (*e.g.*, National Disaster Medical System). In addition to providing this information, this capability needs to provide for:

- Quick establishment of screening/triage at designated primary and alternate medical facilities or emergency centers.
- Hospital “lockdown” (control entry/exit to enforce quarantine or limit spread of contaminants).
- Public education to help citizens function as first-aid or stopgap healthcare providers.
- Personnel and staffing planning across a region.
- Pre-event stocking of needed supplies and pharmaceuticals.
- Identification of needs and inspection of alternate facilities.
- Integration of planning with other organizations and participants.

Current Capabilities:

Currently, distribution of information and gathering of required data is accomplished through faxes, telephone calls, and radio transmissions, which can take 45-90 minutes to complete, even if the effort is pre-planned. This time consuming process hinders the ability of resource managers to meet the first two goals identified above. However, other than for communications and information distribution, technology is probably not the major obstacle to achieving these capabilities.

Emergency response organizations and supporting EOCs have guidance available to them regarding the spectrum of possible events to plan for; however, there is no guidance on how to plan for the specific needs for emergency medical services. This area requires very specialized knowledge that is not traditionally found among emergency planners in an EOC or in responder organizations. There are some plans for mass immunizations that could be somewhat useful as templates, but there is a need to train people on how to plan for these contingencies.

Few localities have identified alternative hospital locations for additional bed space or treatment specialties. Most hospitals have cooperative agreements to transfer certain types of patients to alternate hospitals, but these transfers will overwhelm hospitals very rapidly in the case of a major CBRNE event. There is very limited surge capacity at most hospitals and few have the capability to lockdown to prevent walk-ins.

State of the Art:

Attaining the objectives and goals for this area may be facilitated through assistance from the Centers for Disease Control (CDC) and the Health Resources and Services Administration (HRSA).

CDC-HRSA bioterrorism funding grant programs are available to help state and local governments upgrade public health infrastructure and health care systems to better prepare for and respond to bioterrorism and other public health emergencies. CDC administers public health preparedness awards, which total $870 million. HRSA funds the hospital preparedness cooperative agreements, totaling $498 million. The CDC's guidance this year focuses on seven areas: preparedness planning and readiness assessment; surveillance and epidemiology; laboratory capacity for handling biologic agents; laboratory capacity for handling chemical agents; health alert network and information technology; communi- cating health risks and health information dissemination; and education and training.

The HRSA guidelines for cooperative agreements outline six priority areas: governance; regional surge capacity to handle terrorism victims; emergency medical services; hospital linkages to public health departments; education and preparedness training; and terrorism preparedness exercises.

Several software systems have been developed and used by medical facilities to improve the ability to track and report capabilities through emergency management centers. These systems have substantial overlap with those that will help provide early warning of a biological attack through monitoring of the demand for medical care. (See PHRBAE.1 (*Surveillance and Information Integration Systems*) as well as MR.2 (*Mass Casualty Medical Care Management*).)

Technology Limitations and Barriers:

This capability does not require additional technology development to meet the stated goals. The technologies and software tools exist, but the requirement for hospitals and medical facilities to accumulate and report the data through standardized protocols does not. The barriers are primarily procedural and operational.

Gap Fillers:

A key gap filler is the development of systems with existing technologies for integrating and distributing needed information on hospital and alternate facility capacity and resource availability. The ability to track the information exists, but some hospitals see this information as commercially sensitive, and others see this process as an excessive administrative burden. Thus, the willingness and procedures to share this information should be addressed through national standards

and benchmarks. Planners should pursue the following paths to partially implement this capability:

- Conduct case studies and identify best practices from actual events or benchmarks from effective advances in managing hospital contingencies.
- Build on existing networks. For example, Maryland has a secure statewide health sector emergency data communications system and Facilities Resource Emergency Database (FRED) that is used both for facility resource management and for alerting.
- Evaluate the CDC/Public Health Service report on emergency management tracking systems in Texas, Louisiana, Arkansas, and Oklahoma for feasible pilot programs.
- Integrate with syndromic surveillance efforts. Reporting of hospitals/pharmacies reporting use trends could be expanded to include beds/assets. Many of the same communications links are needed for both purposes. (PHRBAE.1 (*Surveillance and Information Integration Systems*) discusses other efforts as well.)

EMPP.5 – Course of Action Development. *The ability to develop Office of Emergency Management (OEM) procedures, tactics and plans after identification of potential terrorist threats within a locality.*

Providing accurate and accessible information to support contingency planning and response presents a formidable challenge to the emergency planning community. The emergency manager's challenge has always been to acquire enough accurate information to make correct decisions, prioritize the application of resources, and then keep track of the results. Additional complexity derives from the requirement to coordinate response operations in an overwhelming CBRNE event with response undertaken by a variety of agencies with blurred responsibilities. A complex web of government agencies, military organizations, and state and local responding agencies operate within an uncertain organizational structure that needs close coordination. A high degree of organization and preparation is required to support responders' information needs effectively, and success relies on the ability to acquire real time data which change dynamically, integrate it with geographical data, and provide the managers and responders with a continuous view of the status of the situation.

Tactical/operational decision makers (responders) need to have this vast array of data immediately available, generally in a graphical display form. Additionally, there is the need for an organized management information system to support strategic activities (*i.e.*, pre-disaster planning, training and event reconstruction that occur at the EOC).

Goals:

The various interrelationships of data required need to be integrated into several complete decision support systems and management information systems to support tactical planning, response management and damage assessment. The various systems fall into two fundamental components: database systems, and expert systems. The database system serves as a warehouse for the data, and the expert system implements decision support. Linked modules include visualization systems to translate raw data and model outputs, and GIS tools to represent geographically referenced information. Visualization tools are essential for emergency managers to integrate and analyze the complex, massive datasets that will flow from WMD events that most responders and managers expect.

It should be recognized that this functional capability is very closely aligned with the description and goals of EMPP.1 (*Risk Awareness and Assessment*), as well as UIC.4 (*Incident Command Information Management and Dissemination*) and LS.1 (*Logistics Information System*). An effective decision support system should provide:

- Capabilities benchmarked by experienced and fully resourced municipal emergency management agencies.

- Interagency and metropolitan area integration.
- Simulation/exercise evaluation of plans.
- Modeling, simulation, and red-teaming capability.
- Ability to identify and track training and performance needs.
- Indicators for early warning assessment processes and tools (*e.g.*, play-books and target folders).

Current Capabilities:

Technologies exist in this area, but they have yet to be effectively applied to this problem. Little in the way of templates and decision support software has been utilized by responders.

A working system (even if all of the data sets are available necessary to support visualization) must be fully integrated, in order to couple attribute-based dataset queries with high performance visualizations. There are advanced file-based systems that provide a solution to this problem, but there is little implementation at the state or local levels. (These should not be considered technology limitations as much as availability, training, and usability impediments.)

State of the Art:

The state of the art for EMPP.1 (*Risk Awareness and Assessment*) described available software applications that are useful for this functional capability as well. There are several software systems that have been applied to achieving some of the goals listed for this functional element.

Technology Limitations and Barriers:

Despite the apparent merits, most visualization systems generally lack data management support of the scope described by the goals listed above. They offer some built-in support for finding pertinent datasets based upon the attributes of the datasets but generally provide a fairly low-level file browsing or tabular reporting mechanism. Additional complexity is added by diffuse emergency management and response organization personnel who need to collaborate in a multitasking, multistage effort.

Gap Fillers:

Products that could be deployed soon and that would close some gaps in this needed capability include:

- A common standardized distributed database and web server that can be used by federal, state and local emergency planning and response agencies, to provide comprehensive updated data and models relative to anticipated CBRNE threat scenarios.
- A decision support system that provides algorithmic simulation and support for evaluating intervention and response actions, and highlights specific planning and operational issues as a consequence.

EMPP.6 – Establish Emergency Operation Center (EOC).

The ability to establish an effective multi-agency, multi-discipline coordination and information resource center, to support coordination and direction of strategic resource management, communication, logistics, etc. following a WMD event.

In a catastrophe, decision-makers would face a vast amount of disorder and the most pressing need would be for a unified concept of operations that would reduce the disarray among primary responders. With central management overwhelmed in the first few hours, the EOC would be the focus for supporting networks operating somewhat independently without any significant degree of direct coordinated guidance.

Goals:

Responders emphasized the need to "build from the bottom up." This approach provides solid prototypes and operational concepts that have credible support among the responder community that can develop into a synchronized national emergency management system over time. Effective unified command at the local level is the first step in developing a national capability to respond effectively to a major terrorist event.

The objective of a unified concept of operations from a central EOC is to mobilize, deploy and utilize all essential resources and capabilities into an action plan that effectively prioritizes tasks needed in response to a terrorist attack. Coordination, cooperation, and collaboration among the decision-makers requires establishing an EOC capability that can meet the following goals:

- Interoperable communications (up/down/horizontal).
- Current situation and resource status and location.
- Ability to project future operations.
- Database and communications integration.
- Common command system and terminology.
- Seamless integration between EOC and field command units.
- Open architecture and ability to exchange/synchronize datasets among different nodes in the decision-making or management network.
- Rapid communication links to regional and national EOCs, agencies and "trigger points" (surveillance control stations, command posts, etc.).
- Geographical and functional redundancy in other non-proximate location.
- Surge capacity workspace and logistics support.

Current Capabilities:

Each state has some facility designated as an EOC but capabilities, space, and equipment vary widely. Major metropolitan areas have a range of EOC facilities that mirror the range of capabilities at the state level. However, fiscal constraints would make it virtually impossible for jurisdictions to have all capabilities needed to respond to a major event, forcing them to draw on capabilities from many different locations. The scope of mobilization, deployment and utilization needed at theses facilities could be compared to the challenges of planning for continued operation of cities following a limited nuclear attack during the Cold War. At present, in the event of a catastrophic attack, EOC network and response managers would find themselves operating in an environment with the following characteristics:

- Many jurisdictions would lack adequate planning, training, information systems, communications, or response agency associations sufficient for all possible scenarios.
- Most initial responses would be *ad hoc* and depend on system capacities and responder training in place at the moment of the attack.
- Confusion and misinformation would proliferate regarding unknown agents and their effects, public reactions, other response activities, and availability of needed resources.
- Competing priorities, competition for resources and lack of coordination would be endemic among responders, incident commanders, and EOC directors.
- Strict command and control would be impossible as emergency responders followed their instincts in the initial moments following the attack. In the first three to six hours, incident commanders and supporting systems would be hard-pressed to assimilate the scope of impacts and resource needs to issue all of the necessary orders, even if communications were perfect.

State of the Art:

There is a daunting array of operating centers of various sorts at the national level. Only FEMA has developed an effective system of Regional Operations Centers (ROCs) designed to coordinate federal response in support of state and local jurisdictions for emergencies and disasters.

Most very large municipalities, states, and DHS (FEMA) have operations centers that are capable of functioning to achieve the stated goals. The FEMA Regional Operations Centers were designed and equipped specifically to implement the Federal Response Plan and manage the

resource support needs of states following a disaster.

The Emergency Management XML Consortium is developing standards based on Extensible Markup Language to help emergency managers and responders improve data and graphic compression to facilitate and better integrate diverse software and hardware. The consortium is organized under the Standardization Committee of the Organization for the Advancement of Structured Information Standards (OASIS) standards body.

The consortium working on the Standardization Committee has more than 50 members that are supporting the development of the XML schema-based standards. The range of improvements includes unified incident management, geographic information system data accessibility and usage, notification methods and messaging, situational reporting, source tasking, and asset and resource management. Technologists expect to have a clearer and streamlined path to Internet interoperability using this EXML standard by end of 2003.

Technology Limitations and Barriers:

There are no specific limitations to the implementation of existing technologies in the EOC environment. Data transfer and communications are where most technological limitations reside, to include access to telecommunications, cell phone networks, and the Internet during a crisis. Limitations in sharing data and communicating (*i.e.*, equipment interoperability) also have been a concern for many public safety officials for years.[9] Communications interoperability issues, such as those identified after the September 11th, 2001, terrorist attacks between New York City firefighters and law enforcement officers, also extend to the sharing of other digital exchange and integration capabilities where there is not a focused, clearly delineated set of standards for incident management.

There are presently some limitations in storage and display capabilities in individual responder vehicles and even greater limitations in the speed of delivery via wireless means in a networked or Web-enabled mode (especially in the network overload conditions to be expected in an incident). Responders are also concerned with the difficulty in data integration and graphics/data compression, exacerbated by a lack of software standards. Technologists have noted, however, that improved interoperability and speed of data exchange could be gained with standardized coding for the commonly used EXML/XML Web programming language, discussed above.

Gap Fillers:

Templates and training courses to establish EOCs could be very helpful. The federal government might consider establishing local/state/regional EOCs, of which there are currently a few examples.

Because of its complexity, a unified concept of operations requires common response coordination with the strong support by major stakeholders. One option to expand the coordination of multiple agencies from multiple levels is to develop regional operations centers in major cities that are well-staffed and more experienced in the problems associated with a major event. They have planned, trained, and exercised with surrounding counties, states. They are familiar with the integration of federal and military assets.

Emergency managers and unified command systems have made great strides in developing EOCs and operating concepts to address these problems that are likely to occur in coordinating response to a major terrorist incident. Most build on the incident command system. However, the lack of a unifying concept of operations that functions from a capable EOC facility would lead to wasted resources, lives lost and a delayed response. While there is acceptance that a tightly managed response might initially be impossible, a management concept that provides for a well-connected EOC could allow considerable independent action within centrally coordinated guidelines. This could be accomplished through a coherent

[9] Methods for assuring communications connectivity and achieving interoperability are addressed in the NTRO on Unified Incident Command Decision Support and Interoperable Communications

"network of networks" that linked the EOCs of response organizations from many agencies and levels.

EMPP.7 – Facilities/nfrastructure Hardening. *The ability to provide information on mitigation, hardening techniques and response planning to facility managers regarding identified high-value assets and facilities, apply hardening codes (to include retrofit laws and standards) and test and evaluate the hardening effort.*

Goals:

The traditional threat modes that government and military facilities consider for building and equipment protection include hardening measures in the following groupings:

- Penetration shielding from man-portable explosive (thrown explosive, missile, rocket propelled grenade) attack.
- Protection from terrorist/saboteur vehicle bombs.
- Radiation shielding.
- Protection from air bio/chemical contamination.
- Protection from intruders proceeding on foot.
- Shielding from electromagnetic pulses (EMP).

The range of hardening would generally include security, robustness, resilience, and redundancy. The goals for this functional element are:

- Procedures to identify and prioritize high risk target hazards (coordinated with EMPP.3 (*High-Value Target Identification and Monitoring*) above) for hardening.
- Centralized repository of standardized codes and strategies.
- Ability to retain functionality of the structure being hardened, balancing functionality vs. security (cost-benefit analysis).
- Certification of tested and evaluated products.

Current Capabilities:

The capability to conduct risk assessments and engineer hardening in all listed categories is available. DoD and FEMA have studied hardening methods and established protective standards for decades. However, the guidance on what levels of hardening are required is limited and specific to locations that have unique requirements for protection of equipment or personnel, and usually specified in regulations (*i.e.*, prisons, weapons storage, communications centers, banks, etc.). More extensive tools are required, for determining needs and standards for general application at the state and local levels.

State of the Art:

The Department of Defense has many programs that address the needs of the military to protect and defend soldiers, equipment and personnel from attacks of all kinds, including those that might be perpetrated by terrorists.

Technology Limitations and Barriers:

The technologies are mature for assessment, design, engineering and applying physical hardening to facilities to achieve desired levels of protection. The only impediments are methods for credible risk assessment to determine needs for physical enhancement and justification of the subsequent cost for completing the upgrades. Standards for assessment, design, and engineering against chemical, biological and radiological threats are less mature because of the wide variety of the threats and because of limits on our knowledge of lethal doses in real world conditions. Improvements are easy to design but full protection is very difficult to assure; arriving at an appropriate intermediate point would be difficult. Hardening against nuclear blast, fire, and EMP effects is also fairly well understood but impossible at close range.

Gap Fillers:

FEMA provided extensive guidance to states and local governments for analyzing facility protection and attack resistance during the Cold War era from the late 1950's through the mid 1990's. FEMA provides standards for EOC survivability

and hardening enhancement for existing structures to serve as shelters, command centers, and alternate government sites. Each state had a Facilities Engineer staff position that was 100% federally funded. This information and guidance is still available from FEMA archives and many states retain the regulatory and guidance information. The Department of Defense and communicable disease laboratories have methods, techniques, standards and protocols for construction of facilities that are effectively resistant or hardened to prevent penetration or release of biological threats. The cost and operational viability of such facilities in the CBRNE terrorism context is highly questionable, however. While the ability and technology exists to construct or harden a facility to the standard of a Level 4 Bio-Lab, the functionality of such facilities would be severely limiting and it is doubtful that a cost/benefit analysis would support application except in rare instances. Jurisdictions that desire hardening to the blast overpressures of the nuclear attack survivability standards that FEMA defined or that the CDC promulgates for design of a Level 4 laboratory can acquire and use this information to develop hardening standards and procedures to the extent of the resources available to support the associated costs.

Emergency Management Preparation and Planning Response Technology Objectives (EMPPrto)

The Emergency Management Preparation and Planning capabilities described above are not generally dependent on new or emerging technologies. Rather, capability increase will come primarily from the identification and integration of best-of-breed software and procedures, guided by standards developed specifically for emergency management preparation and planning at the local level. Continued improvements and enhancements in technologies are still important, however. In most cases, meeting needs and goals is dependent on development of standards, application of operational/procedural methods, acquiring existing data sets, man-hours to enter data for specific sites, and/or making fiscal and training commitments to implement existing technologies. The discussion of EMPP Response Technology Objectives expands on these combinations, and highlights existing technologies that can be improved or made more feasible for implementation.

The diversity of responder organizations and local and state authorities employing disparate systems of command, control and coordination presents a significant obstacle to effective implementation of existing technologies and best practices. Data warehousing and knowledge management systems that have been effectively implemented within some military organizations, federal agencies, or large cities are not compatible with systems that are generally in widespread use, thus hindering the ability for multi-agency, multi-level response in a complex environment. Commonality and similarities among crisis management systems locally, regionally, and nationally are needed to foster effective joint efforts. Preparedness for effective response management is most effective when it is simple, flexible, and standardized.

In the hours immediately following a major event information management and decision support systems must provide for decentralized management that permits a fair degree of autonomy to the functional networks collaborating in the response. The rapid linkage of these compatible systems is needed to ensure the devolution of information and management, and to establish a common operational picture. Because of the complexity of implementing such systems, acceptance of hardware and software standards needs the enthusiastic support of major stakeholders from local, state, and key military/federal agencies. Most entities recognize the problems and have been working on finding solutions. The most immediate need is to create a continuing process that builds on the insight of key stakeholders. This is consistent with the need to "build from the bottom up" in a process that provides concrete pilots projects led by credible federal-level agencies that could harmonize this unified, national concept for support.

EMPPrto.1 – Risk Awareness and Assessment Decision Support Technology Demonstration

Objectives:

Determine selection criteria for software systems that are effective, and metrics for assurance that critical data sets will be available to responders and sustainable. Determine "best-of-breed" in useable collaborative decision-support systems that promote effective emergency response planning. Create benchmarks for integrated systems that will consolidate the stove-piped risk and impact assessment models currently available. Demonstrate an integrated, effective set of shared tools that monitor the urban environment and provide enhanced near real-time situational and integrated data from disparate sources into a single coherent view to support disciplined decision-making.

Payoffs:

The development of systems that can accomplish the stated objectives will allow the nation's responders and emergency managers to initiate a response with confidence that their incident situational awareness is valid. Follow-on responders and off-scene managers will have a common view of the tactical arena and collective basis for crisis action and strategy development for consequence management. This demonstration should result in a capability that helps free the crisis management team from time-consuming and tedious data assessment and filtering, permitting higher-level situational assessment and rapid response to changing events.

Challenges:

Although the technologies are generally available, the challenge is to design the linkable networks to overcome the traditional lack of compatibility of many off-the-shelf proprietary software packages, data sets, and digital maps. There is a technical challenge in implementing the digital architecture and supporting software which must accommodate a wide range of existing equipment and systems. Those capabilities have been demonstrated in exercises and tests, but the challenge remains to commit the time and effort for initial and sustainment training to ensure usability of relatively complex software.

Milestones/Metrics:

The RTO should be oriented around a demonstration project following selection of software, training of responders/EOC personnel, and establishing multi-agency/multi-level interoperability, including the following milestones:

FY2004: Pilot program to define requirements for software integration originating at the local level (bottom-up approach).

FY2005: Select demonstration sites that are small to medium sized cities that have a real-world pre-planned event.

FY2006: Demonstrate integrated technologies in actual use with live data and information flow to evaluate capabilities implementation and improvement.

Technologies should demonstrate, in a carefully constructed series of exercises, ability to meet responders' confidence in the usability, interoperability, and capability of accomplishing the stated goals.

The Defense Threat Reduction Agency, National Institute of Justice, and the Office for Domestic Preparedness already have extensive experience with such assessment software.

EMPPrto.1 – Budget in Millions

Thrust	2004	2005	2006	Totals
Decision Support Technology Demonstration	$2.5	$4	$3.5	**$10**

EMPPrto.2 – Electronic Transcript Smart Card. The advent of the Internet and its steady development from a text-only medium to an expanding multimedia communication system has offered new and diverse opportunities for training at convenient times and places. The expanding range of possibilities requires training managers to be proactive in the development and use of technology in the teaching-learning process. They must become involved in the development process to ensure that it is the educational needs that are driving the development

of technology, rather than vice versa. These responsibilities can be supported by technologies that allow training and response managers to verify responders' proficiency and currency in specific skill sets and training requirements.

Objectives:

Demonstrate, for standardization and acceptance, a digital smart card/chip "electronic transcript" system that securely verifies identification, levels of training/certification, and currency, for the multitude of responders that converge on the scene of a high-visibility CBRNE event.

Payoffs:

Immediate verification of credentials is essential to make effective use of volunteers and mutual aid that may arrive in a chaotic fashion. The tracking of the individuals for safety and their qualifications is an overwhelming task for incident commanders. Use of such smart cards, with chips programmed to turn on when the wearer crosses a designated perimeter, would give the on-scene commander a rapid, accurate, and verifiable picture of resource and skill availability, and ensure the qualifications of each responder at the scene. This objective could ultimately be combined in a synergistic way with the responder personal locator technology that is the subject of UICrto.1, to enable safety monitoring and accounting throughout the event.

Challenges:

The GPS-enabled smart card technology to achieve the objective is available but it is not in widespread use. The GPS feature may not in fact be necessary in an early version that would rely on the inherent short distance of the card/reader combination for rough location. This is a low-risk demonstration project to benchmark systems that can ensure interface and display capabilities in the emergency responder communities. The challenge is to gain acceptance of the use of technology that tracks movement and location of individuals. In some implementation scenarios, responders saw personnel tracking as an invasion of privacy or violation of union rules. Procedures and policies that address these concerns have been demonstrated in Boston, Massachusetts and Prince William County, Virginia.

Milestones/Metrics:

Milestones should focus on demonstration projects in three sites (large, medium, and small jurisdiction) following selection of software, evaluation of hardware, training of ICS staff, and responders to employ the "smart card" technology in a multi-jurisdiction response exercise.

Technologies should demonstrate, in a carefully constructed series of exercises, ability to meet responders' confidence in the usability, interoperability, and capability of accomplishing the stated goals.

FY2004: Research existing technology; define requirements for information to be tracked; specify/the minimum equipment specifications; select software to implement the smart card technology.

FY2005: Select three jurisdictions for demonstration sites that test the technology in the full range of response; demonstrate tracking technologies in actual use with live data and information flow to evaluate capabilities implementation and identify shortfalls.

FY2006: Evaluate systems for effectiveness.

FY2007: Produce strategies, best practices, and technology benchmarks/minimum standards for technology implementation.

EMPPrto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Electronic Transcript Smart Card	$2.25	$3	$1	$0.75	**$7**

EMPPrto.3 – Alternate/Mobile Hospital Contingency Management

Objectives:

Develop standards based on case studies, benchmarking, and best practices in use for managing hospital/medical contingencies. A formal study of software systems (perhaps by CDC or Public Health Service) is needed, to determine the existing capabilities, feasibility of expansion, and the

inclination of hospitals to support the reporting requirements.

Payoffs:

Quick implementation of critical resource reporting of hospital and medical resources in common database formats for decision support by incident commanders, emergency responders, and emergency managers.

Challenges:

This is a very low risk enterprise that uses readily available existing technologies and COTS software to accomplish the desired goals. Benchmarking and best practices will be demonstrated in a relatively straightforward endeavor that studies the implementation in three to five municipalities using existing systems.

Milestones/Metrics:

Review and evaluate software to use in a demonstration project to test capabilities for coordinating medical resource availability and prioritization. This demonstration project should follow selection of software, training of responders/EOC personnel, and participating hospitals in two jurisdictions. Project completion includes the following milestones:

FY2004: Pilot program to define requirements for software integration, and demonstrate implementation, originating at the local level with jurisdictions that have volunteer hospital participation (bottom-up approach).

FY2005: Demonstrate technology and evaluate system usage, in two jurisdictions that have hospital/medical facilities with existing computer-based resource tracking capability, with integrated technologies in actual use using live data and information flow to evaluate capabilities implementation and identify shortfalls.

FY2006: Analyze and define strategies/best practices for technology selection (benchmarking) and implementation.

Technologies should demonstrate, in two carefully constructed exercises, ability to meet responders' confidence in the usability, interoperability, and capability of accomplishing the stated goals.

EMPPrto.3 – Budget in Millions

Thrust	2004	2005	2006	Totals
Alternate/Mobile Hospital Contingency Management	$1.75	$0.75	$0.75	**$3.25**

EMPPrto.4 – Course-of-Action Development System.

Computer-based decision support and information management technologies can assist the emergency planning/response community in achieving a higher level of sophistication in information assessment, integration and manipulation. An effective decision-support (or *course of action development system*) should synthesize information in a manner that facilitates and speeds up the decision-making process and allows for the development of databases that reflect the full spectrum of the various organizational modes, resources and capabilities. Policy and procedure integration with constant sustainment training is needed for this capability to find broad acceptance and implementation.

Objectives:

Software integration to link existing GIS, modeling, planning, flood and incident management systems, National Crime Information Center information, Radiological Emergency Preparedness systems, and specialty databases (*e.g.*, California's earthquake-related systems), with existing decision support programs. The sponsorship of this effort should fall to the organizations already heavily committed to developing systems that span the local, state, federal, and military multi-level response structures. Those two national organizations are the Defense Threat Reduction Agency (DTRA) and Department of Homeland Security (FEMA). The CATS system that is sponsored by DTRA is particularly well-suited to build on for benchmarking and standards for integration and interoperability, and the FEMA HAZUS-MH system is the most capable GIS-based natural hazards system.

Payoffs:

A course-of-action development system will help incident commanders and EOC officials make better decisions more efficiently and in better coordination. Developing interoperability standards will facilitate the DHS policy for EOC regionalization and encourage others to make the commitments to cost, training, and strategic planning necessary to commit resources and implement compatible EOCs.

Challenges:

There are no significant technological challenges to pursuing these goals. Risk is minimal.

Milestones/Metrics:

The salient effort is focused on a proof-of-concept demonstration project that provides for multi-agency, multi-level linking of compatible systems that are already in use. A unified approach by organizations "owning" the software must define protocols for exchange of compatible data sets and visualization outputs. The ultimate goals are to select the most capable and compatible software, select viable demonstration sites for a tiered exercise, train responders/EOC personnel and other participants, and demonstrate multi-agency/multi-level interoperability. The project includes the following milestones:

FY2004: Evaluate candidate software that is available and in effective use; define integration and data-exchange protocols that will be compatible with system capabilities at local levels.

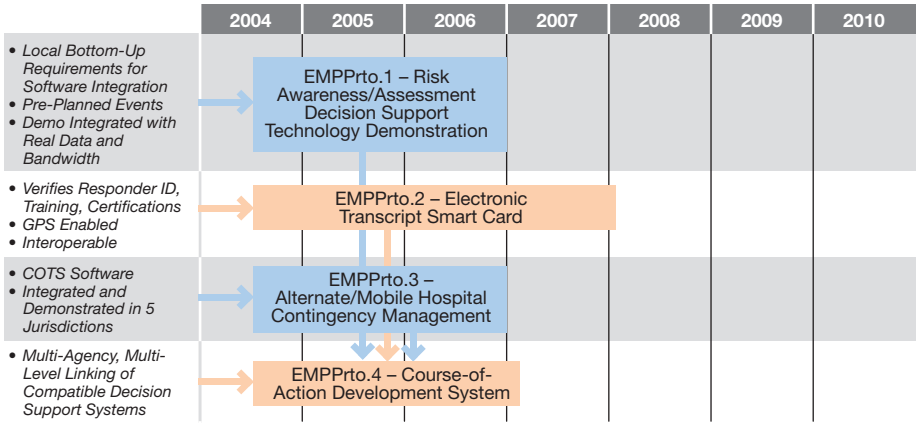
FY2005: Define minimum equipment criteria; select equipment for use in testing; deploy software and equipment for exercise and train participants.

FY2006: Select four demonstration sites that are representative of the full range of local response capabilities (one large, two medium, one small jurisdiction); demonstrate integrated technologies in actual use with live data and information flow to evaluate capabilities implementation and areas for improvement. Evaluate effectiveness of systems.

The technology demonstration will facilitate responder and command-level confidence in the usability, interoperability, and capability of accomplishing the stated goals.

EMPPrto.4 – Budget in Millions

Thrust	2004	2005	2006	Totals
Course-of-Action Development System	$3.5	$8	$6.75	**$18.25**



Emergency Management Preparation and Planning Technology Roadmap

Chapter VII

Medical Response (MR)

Chapter Chair: Dr. Stephen Kornguth
Chapter Coordinator: Michelle Royal

Definition

Medical Response is the capability to provide rapid, effective, safe treatment of persons exposed to CBRNE threats. This is achieved by mobilizing, deploying, and sustaining a safe field medical response in full coordination with hospitals and public health infrastructures.

This section is complemented by the Public Health Readiness for Biological Agent Events (PHRBAE) National Terrorism Response Objective (see Chapter VIII), which focuses on capabilities needed specifically for response to biological threats.

Operational Environments

The type of event or threat scenario proved to be the most relevant way of defining the variety of operational environments for medical response. Therefore, this NTRO's Operational Environments are: chemical, biological, radiological, nuclear, and high explosive/incendiary. However, in most instances the effects of a nuclear explosion on survivors amount to combinations of exposure to radiation, heat, fire, and blast (though probably on a larger scale). Thus, the nuclear operational environment calls for combinations of capabilities needed for the radiological and explosive/incendiary operational environments. For this reason, within some functional capability areas, the 'nuclear' operational environment is considered not applicable because all the needed capabilities are included within the radiological and explosive/incendiary operational environments.

The capabilities required for medical response to a biological or radiological incident differ from those appropriate in a chemical, nuclear or high explosive incident. In biological and radiological events, there is a longer time delay between release of the agent and manifestation of its consequences among an affected population. The continued threat of exposed persons to others persists because of the infectious quality of biological agent or prolonged half-life of the radiological agent. The effects of nuclear, chemical and explosive materials on a target are apparent within seconds to minutes of the event. Radiological materials will manifest their adverse effects on a target within hours if the dosage is high; it may take weeks to years to observe the full consequences of the threat materials at lower doses. Humans, animals, or plants will manifest clinical signs typically seventy-two hours to eight days after exposure to a biological threat agent. Because of the delay between exposure and appearance of clinical signs, the type of emergency responder will differ and the management of the high threat situation will require strategies that differ from other CBRNE events.

There are two distinct timelines for recognition of an event: immediate and delayed. If sensor systems that detect threat agents are present at the time of release, immediate action may be taken by authorities in proximity to the event. Such action includes securing the perimeter followed by treatment of exposed persons with appropriate antibiotics, antivirals, and anti-toxins. However, the more likely response to a biological event (and to low-level radiological and chemical events) will be along a delayed timeline, where the dispersal of the threat agent will not be detected at the time of release. Responders may not recognize the occurrence of an event until after the first appearance of clinical signs

inconsistent with normal patterns of illness in the community. This will occur typically three to eight days after release of the biological agent, or possibly longer in the case of a low-level radiological incident. The emergency responder in this situation will be the health care provider in an emergency medical service environment, an emergency room, a private physician, the pathologist, a pharmacist or a family member.

Diagnosing and distinguishing an illness as a result of either an emergent disease or bioterrorist activity will be frustrated by two issues: 1) many illnesses appear similar to common flu at early stages (enteric or respiratory signs), and 2) the process of differential diagnosis requires the diagnostician first to rule out the most probable causes of illness before considering unlikely causes.

There are three important timeframes related to a biological threat: pre-event, minutes to hours surrounding the release event, and four or more hours post-event. Protective measures in the pre-event period and during the release phase include vaccination, storage and maintenance of vaccines, antivirals and antibiotics, body-cover similar to that used in surgical suites, face masks that cover the mouth, nose, ears and glasses. In the absence of skin abrasions or puncture wounds, biological threat agents (*i.e.*, viruses, bacteria, fungi and toxins) will generally not penetrate intact skin (with the exception of cutaneous anthrax). They may be ingested, inhaled or injected. After the first four hours antibiotics, antivirals and vaccines will be required. Those persons exposed to agents should be placed in isolation. Care providers and emergency responders will require face masks and gloves. Washing hands with detergent or diluted bleach is required and contaminated clothes should be removed and contained at a safe designated site near the incident.

Needed Functional Capabilities and Priorities

The functional capabilities needed for this NTRO, in priority order, are:

- Mass Medical Prophylaxis
- Mass Casualty Medical Care Management
- Individual and Collective Protection of Health Care Personnel and Facilities
- Rapid Clinical, Environmental and Veterinary Field Assessment.
- Medical Response to Public Affairs
- Modeling of Exposure/Casualties for Location and Numbers
- Definitive Decontamination
- Medical Staff Surge, Re-Supply and Proper Accreditation
- Telemedicine in Support of Surge

The functional capabilities are presented in priority order based on responders' input in workshops and field interviews conducted during the earlier phases of this effort. The functional capabilities were subsequently modified and validated in workshops involving both responders and technologists. The first three (*Mass Medical Prophylaxis* (MR.1); *Mass Casualty Medical Care Management* (MR.2); and *Individual and Collective Protection of Health Care Facilities and Personnel* (MR.3)) were regarded by a strong consensus as the highest priorities in this NTRO.

It should be noted that this NTRO originally considered the functional capability *Therapeutics and Treatments in Dangerous Environments*. This functional capability was originally considered lowest priority of the NTRO. After further consideration, responders agreed there was no real need to pursue this capability because they could not foresee any scenario where treatment will be given in the "hot zone." Current strategy involves the removal of exposed persons from the hot zone to an adjacent clean area and subsequent removal of clothing and washing of exposed persons. Therefore, this functional capability was eliminated from the list of needed capabilities for this NTRO.

The responders believe that marked improvement is needed in the rapid detection of agents in hot

zones and of persons exposed to threat agents. They also believe that new approaches are necessary for administration of prophylaxis to large numbers of persons. A high priority was placed on developing tools for looking downrange at an incident to identify health status of victims and detecting threats in the environment. This is addressed in part in Chapter III (DIDA) and Chapter IV (UIC). A related high priority is availability of a voice-activated documentation assessment tool to link emergency responders to hospitals and clinics via the Internet.

Medical Response

Functional Capabilities	Operational Environments: Chemical	Biological	Radiological	Nuclear	High Explosive/ Incendiary
1. Mass Medical Prophylaxis					
2. Mass Casualty Medical Care Management					
3. Individual and Collective Protection of Health Care Facilities and Personnel					
4. Rapid, Clinical Environmental and Veterinary Field Assessment					
5. Medical Response Public Affairs					
6. Modeling of Exposure/ Casualties for Location and Numbers					
7. Definitive Decontamination					
8. Medical Staff Surge, Re-Supply and Proper Accreditation					
9. Telemedicine in Support of Surge Requirements					

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

The discussion of the individual capabilities is related to the needs identified. Several of the essential needs do not require novel technology development (*e.g.*, capability to distribute vaccines, antivirals and antibiotics) but rather require an adaptive change in administrative policy and culture. Other needs do require technological innovation (*e.g.*, modeling dissemination of aerosols based on meteorological data at low altitude). While technological advances are required in this area, modification of public attitudes and administrative structures will also be required if success is to be realized.

Overall State of Technology for Medical Response

The matrix below shows a pattern of moderate to high technological challenges in meeting the needs of medical responders.

MR.1 – Mass Medical Prophylaxis. *The ability to provide mass medical prophylaxis (including antibiotics, antivirals and vaccinations) to persons exposed to biological agents, and to provide appropriate pharmaceuticals or protective materials to persons exposed to chemical, radiological or high explosive incidents.*

This functional capability assumes that knowledge of an incident is timely enough that prophylaxis is administered at or near the scene and therefore can mitigate danger to potential victims and responders. In the case of biological or radiological agents, the window for recognition of an event is about 24 to 96 hours post exposure; for chemical agents, the window is seconds to minutes.

Goals:

This functional capability includes the following goals:

- Identification of at-risk population.

- Protection of population from developing illness after a CBRNE event.
- Identification of appropriate prophylaxis and contraindications.
- Improved delivery methods.
- Strategy development for distribution of material (including staffing, logistics, facilities, etc.).
- Expedient/efficient acquisition, distribution and administration (to include tracking) of prophylaxis.
- Strategies for managing pharmaceutical stockpiles.
- Security, force protection and social control.
- Methods to model and test systems in order to improve preparedness for mass prophylaxis eventuality.

The key to this capability is to detect the presence of threat agents at the earliest point after dissemination, to identify the population at highest risk, and to devise a plan to administer protective medication. The detection and identification of threat agents requires sensor technology as described in Chapter III (DIDA). (See also PHRBAE.1 (*Surveillance and Information Integration Systems*), PHRBAE.2 (*Rapid High-Throughput Clinical Assessment and Testing*) and MR.4 (*Rapid Clinical Environmental and Veterinary Field Assessment*).) The identification of the "at-risk" population includes identifying those in the immediate vicinity of the release of agent and others with particular susceptibility to the threat agents (such as the immuno-deficient, aged, or those with chronic disease). This functional capability probably requires specialized demographic databases.

The goals point to a system that merges knowledge about the ongoing incident, previous knowledge about prophylaxis procedures and protocols and modeling and simulation to provide a knowledge base that responders can use to manage a mass prophylaxis operation. In addition, this functional capability establishes a need for new rapid delivery techniques. Improved delivery techniques require development of strategies for distribution (including staffing, logistics, facilities, etc.), expedient and efficient acquisition, and administration (to include tracking) of pharmaceutical stockpiles.

Improved methods have been established for security, responder protection and social control in the event of a CBRNE incident. However, desk-top drills conducted across the nation continue to reveal shortcomings in the system. To improve the capability of the nation to minimize adverse consequences from a CBRNE attack, an additional goal of this capability is development of new methods to test the readiness of systems for mass prophylaxis.

The development (as opposed to management and delivery) of novel prophylaxis to improve protection against some agents is implied in this function. However, this has been outside the scope of Project Responder. Therefore, this functional area is limited to the management and delivery of prophylaxis.

Current Capabilities:

There is no technology in use for rapid identification of at-risk populations. Systems that use real-time information about an attack do not yet exist because that information has not been previously been available. The federal government and some cities are now deploying the kind of sensor systems that could provide that information, on an experimental basis, but more development is required.

With regard to identifying appropriate prophylaxis and contraindications, current studies on the human genome are anticipated to provide information regarding which individuals are most susceptible to adverse responses to antibiotics and other chemicals. It is not possible now to determine which individuals are most susceptible to adverse clinical response to vaccination.

Delivery methods have not changed their basic technology in years, but policies have become more conservative and less supportive of mass

prophylaxis. Auto-injectors and reusable syringes are still the fastest means for delivery. But under current administrative policies and procedures, it has been estimated that approximately 50,000 to 100,000 persons could be vaccinated for smallpox per day in the U.S. according to the Center for Disease Control. Compare this with the vaccination of five to six million in two weeks in New York City in 1947. The change is a consequence of the large number of immuno-deficient individuals today (*e.g.*, organ transplants, AIDS) and the litigious nature of society compared with that in 1947. Difficulties in mass vaccination are further evidenced by the large number of health care workers (90%) who have refused vaccination with the smallpox vaccine. This indicates that even knowledgeable workers do not perceive the risk/benefit ratio of vaccination to be beneficial at this time. Immunization of the population in an urban area the size of New York or other metropolis could require as much as seventy days. By contrast, other countries estimate that a population of five million persons can be immunized in ten days. The problem is therefore more social and political than technological.

Chemical, radiological, nuclear and HE threats are not readily managed by prophylaxis. Ready availability of anti-nerve gas antidotes (acetylcholinesterase inhibitors) can mitigate the effects of exposure; inappropriate use of the antidote however is associated with adverse clinical effects and therefore contributes to the social and legal issues mentioned above.

State of the Art:

Technology currently exists for more rapid delivery of prophylaxis, and for tracking the administration of pre-event and post-event treatment. Marked improvement is needed in rapid administration of prophylaxis for chemical and biological threats as such threats emerge. New tools to monitor and track administration of treatments are also needed.

Elements of the technologies that will enable the goals are emerging today. Smart sensor networks are being developed by the Department of Defense. The Department of Homeland Security is investigating the use of urban mass transit monitoring systems and other fixed arrays as a basis for understanding the urban environment. Demographic databases with GIS registration are being deployed, and data mining of 9-1-1 systems is spreading. Systems that provide event-driven treatment management and bar-coding tied to medical records are also being developed.

Technology Limitations and Barriers:

There are few major technical barriers to increasing our ability to administer antidotes to biological, chemical and radiological agents. The largest technical barrier is the ability to integrate disparate databases. However, the primary limitation is the lack of an administrative infrastructure able to deal with licensing of personnel who are not physicians or are from another jurisdiction. The fact that almost all countermeasures to biological, chemical or radiological threat involve some level of morbidity raises the likelihood of litigation. Rapid determination of at-risk populations is reliant on sensor systems. Therefore, the primary technology barriers to providing this capability are similar to those described in Chapter III (DIDA).

Gap Fillers:

The primary gap filler would be the development of a knowledge base with decision aides, templates, and management support for responders to use to manage a mass prophylaxis operation. The system would integrate existing and future databases to provide access to situational awareness. In addition, a program needs to be created that will address a more rapid delivery system with significantly higher throughput rates

MR.2 – Mass Casualty Medical Care Management. *The ability to provide automated support for handling large numbers of casualties being cared for in many geographical locations and with a wide variety of injuries within likely terrorist scenarios. It includes triage and hospital care.*

The emergency responders placed a high priority on developing an ability to look "downrange" at an incident to allow remote triage and to provide

appropriate support tools for the on-scene responder, similar to those discussed in the previous section. This capability would allow remote sensing of vital signs (*e.g.*, blood pressure, pulse, blood oxygenation, dilated pupils and panic levels). When coupled with a voice activated documentation headset to remotely link vocally documented assessment with text/cathode ray tube (CRT) screen, staff at remote hospitals will be better able to evaluate crisis situations. All this would be part of an automated system to manage the treatment and keep track of the casualties. This capability should be interoperable across all agencies likely to be involved, at least on a regional basis (if not national) and used on a daily basis.

Goals:

The goals for this functional area include:

- Ability to monitor a patient's progress through the system in order to keep track of where people are and treatment updates; linked into a common operational picture for deployment by emergency responders.
- Ability to attach to patients.
- Capable of identifying triage priority, clinical status and personal information; and remotely transmitting it in real time to a common operational picture available to command, EOC, hospitals and other key personnel.
- Medical operational picture containing real-time information about the resource status and patient care capabilities of the local system to command post/EOC (see also EMPP.4 (*Alternate/Mobile Hospital Contingencies*)).
- Development of strategies and systems for distributing personnel resources in massive casualty systems.
- Management of some critical patients simultaneous with triage.
- Biosensing.
- Expert systems to provide appropriate treatment strategy to emergency medical services (EMS) and other responders.

A key goal is the development of technology to monitor a patient's progress through the system in order to keep track of patients' locations and treatment updates. As discussed in the previous section, the management of large number of casualties is one of the biggest problems facing responders. The management system envisioned by this set of goals would certainly overlap with the requirements described in MR.1 (*Mass Medical Prophylaxis*), with greater scope. The goal which differs here is the ability to sense vital physiological information without direct contact (*i.e.*, non-invasive). Responders referred to this as the "triage tricorder." Once acquired, physiological information could be remotely transmitted, in real time, to provide a common medical operational picture made available to command, EOC, hospitals and other key personnel. The biosensing tool is similar to that described in Chapter III (DIDA). Decision support technology to develop triage strategy can emerge from this approach.

Current Capabilities:

At the present time, there are multiple existing systems being used to identify and track victims at an incident site. These systems are primarily manual (*e.g.*, names are taken and entered by hand) and the resulting data sets are not standardized nor linked to other users. Common operational picture systems exist in the military and those systems do integrate medical situational information. The military systems would need to be adapted for civilian use. No capability currently exists in the field to remotely sense physiological characteristics. Some voice activated/recognition medical documentation systems are being deployed in the clinical environment but not in the field. Current voice recognition technology does not work well in noisy environments. Terrorist events will most likely be noisy and chaotic.

State of the Art:

The use of bar codes to track moving items or stockpiles of food is well established at Federal Express and major food stores. Many prototype systems are under development to provide information continuity between emergency medical services and hospitals. The State of Maryland has a prototype program for formatting triage sheets to electronic forms and reporting this information to incident command system for assigning beds. A commercially available software package from Cerner allows the rapid capture of clinical data at the time of patient entry into the system. The DREAMS (Disaster Relief and Emergency Medical Service) project in Texas also utilizes electronic data sets obtained at an incident site to provide a common operational picture to distant medical care providers. The Virginia health care system provides emergency room facilities with medical data from an ambulance, via radio frequency transmission.

Technology Limitations and Barriers:

For this capability to come to full fruition, every health care organization that can potentially become involved in an incident needs to have the system or be interoperable. This presents not only a technical challenge to successfully integrate both new and legacy systems, but a policy and administrative challenge to establish and implement national standards; not to mention cost issues.

Current systems have yet to be tested in a truly mass casualty situation where tens of thousands of victims need to be managed. It remains to be seen what technical difficulties emerge from that scenario. The ability to develop voice recognition systems that can operate effectively in very noisy environments has yet to be realized.

Gap Fillers:

Some elements of programs that should be considered to fill gaps include:

- Voice activated documentation software packages which will permit electronic (remote) information transfer between an incident site and medical management authority, EOC or incident command; the information could be converted to text on a CRT screen.
- Automated casualty management system using bar code technology or radio frequency tags. The system would track patients and their medical information and relay the information back to incident command. This could also be used for syndrome information and analysis.
- Expansion of the physiological monitoring program recommended in DIDA to include this area's bio-sensing needs.
- Systems built for everyday use, not just catastrophic incidents.
- Standards developed and accepted by user communities on a regional and national basis. (The standards must then be integrated into everyday operations so the user community is familiar with the procedure. An Internet-based system is one way of a chieving some standards and to have a robust communications.)
- Ability to train on the system. The inclusion of simulation and virtual reality elements to train while operating the system will be important (e.g., embedded training). (See EMPP.2 (*Mission Rehearsal, Simulation, Embedded Training and Distance Education*).)

MR.3 – Individual and Collective Protection-Health Care Facilities and Personnel. *The ability to protect medical care personnel and facilities (to include field hospitals and triage areas) from CBRNE hazards.*

In the event of a CBR incident, there will be a need for automatic lockdown mechanisms in health care facilities. This is required to diminish the risk of disease to patients at the hospital that are in a pre-existing state of compromised health. The automatic lockdown may be expected to reduce security needs and release responders to undertake other critical missions. Field hospitals would be established to further reduce the risk of

disease dissemination to compromised patients. (See MR.2 (*Mass Casualty Medical Care Management*) and EMPP.4 (*Alternate/Mobile Hospital Contingencies*).) Although technology is an issue, isolation of patients and establishment of field hospitals also involves many policy decisions (*e.g.*, financial allocations, sources of field hospital, routing of critical care patients).

Goals:

The following goals are an indication of what capability is needed in this area:

- Sensor-based, automatic, real-time, secure lockdown systems (*i.e.*, double-door systems).
- Over pressure, filtered air.
- Capacity for isolation.
- Adequate security for site and personnel in the case of a lockdown, supported by rules of engagement (not generally technology enabled except for where manpower can be replaced by barriers with trusted access systems).
- Proper respiratory protection that allows field and hospital medical personnel to see and communicate with the victims (covered in Chapter II (PPE)).
- One-size-fits-all respirators which are easy to use and not bulky. Ease of operation, storable over long term, can be worn for a long time without taxing the responder (covered in Chapter II (PPE)).
- Airlock and bubble to provide containment and safe operations (addressed in Chapter VIII (PHRBAE)).
- Technical evaluation of hospital design which provides ways for people to be assessed without contaminating large numbers of people (not primarily technology-enabled).

As indicated by the parenthetical comments, a number of these goals are being addressed in other NTROs. Still more are not strictly technologically enabled, although some may benefit from the application of mostly off-the-shelf technology (such as in the case of the security goal). It would be most effective to have technical evaluations of hospital designs prior to construction of new facilities so as to enable care of affected persons without contaminating large numbers of people. The development of national standards similar to building codes would be necessary.

Current Capabilities:

At the present time very few, if any, hospitals have a security force capable of locking down the facility. Bio contagion in hospitals is a real problem; nosocomial infections are commonplace in most urban medical facilities. Very few hospitals have any capability to house patients with highly infectious disease. Even those that do have such capability can manage only between ten and forty patients. Many of those hospitals are located in remote areas and present a challenge in transporting patients from an incident site to the facility. Therefore, although the technical ability to treat patients with highly infectious disease or chemical exposure exits, the ability to manage a major attack with associated large numbers of victims remains unaddressed. The low probability of such an attack diminishes the likely allocation of local resources. The high consequence of the event, however, requires novel approaches and solutions. Facilities around the country exist for management of patients with highly infectious disease or with chemical agent exposure. Examples include Ft. Detrick, the University of Texas at Tyler, and the Johns Hopkins University. All the technologies needed to create this capability exist in a commercial off the shelf mode. However, the expense of integrating the capability in existing hospitals will be prohibitive. There are also a limited number of field hospitals in the Army (*e.g.*, Natick) and Air Force for treatment of individuals in conditions of isolation.

State of the Art:

Most of the relevant state-of-the-art technologies reside in the military. For individual protection of health care providers, military medical personnel use the same gear as soldiers. Some of the military hospitals and labs have been fitted with

isolation units that are meant to deal with the treatment of any infectious diseases, including those that are bio-warfare threats. Natick Army Research & Development Center has developed field-deployable hospitals (and other enclosures) built to protect health providers and patients from chemical and biological threats. Some hospitals have built-in protection fields in their triage and emergency room areas. However, there seems to some difference of opinion as to the effectiveness of the methods used. Lack of standards for emergency responders is a problem.

Technology Limitations and Barriers:

The major limitation and barrier in establishing protected facilities is not technical, but financial. The low probability of an attack, even with high consequences, limits enthusiasm for major outlays of funds, especially by local governments. In addition, a large portion of the country's healthcare facilities are private sector entities that must be concerned about the financial "bottom line." Thus, there are very limited resources to finance the required changes. In cases where tens of thousands of victims will need treatment, alternate facilities in schools and other government owned buildings will probably be converted into temporary hospitals. The decontamination of these buildings after use and the public acceptance of assurances that re-occupancy of the buildings will be a very low risk will raise new issues. As an example, reutilization of schools may be problematic if public perception exists that the schools may be unsafe. The inability to use postal facilities that were contaminated by anthrax after clean-up, and the utilization of schools that had reported high levels of asbestos, are two examples of the difficulties regarding community acceptance of decontaminated structures. As stated above however, these are essentially policy and social issues, not technical. It would help to have a better understanding of the risks at low levels of contamination, and assays that detect those low levels. Chapter III (DIDA) recommends work on sensors that would help in this area.

Gap Fillers:

From technology standpoint, technologists and responders agree that the technology is available to meet this needed capability. The deployment of that technology is a funding and policy issue, and therefore no gap filling programs are offered. However, the need remains, and the federal government should study the situation with a view toward determining whether federal funding and policy initiatives are needed to create this capability.

MR.4 – Rapid Clinical, Environmental and Veterinary Field Assessment. *The ability to assess environmental, human and animal data relating to the existence of biological, chemical or radiological threat.* This assessment will assist responders in medical triage and diagnostics.

There is an unmet need to have minimally invasive, rapid diagnostic tools that can be linked to dynamic models of chemical, biological or radiological agent dispersal, and the clinical appearance of disease/morbidity/mortality. These tools would support the treatment and management of thousands of victims.

Goals:

- Rapid diagnostic tools to safely and accurately detect and identify injuries or illnesses.
- Link remote responder to reach back to a specialist for diagnostic support (telemedicine–video and data link/distance triage).
- Linked in real-time to dynamic models, surveillance systems to acute care.
- Broadened multimedia training to expand knowledge among all responders.

These goals again speak to the need for a minimally invasive field diagnostic tool that provides, among other things, the capability to reach back to a specialist for diagnostic support. The linkage must be available in real time and allow the emergency responder to access dynamic models

of disease dissemination and surveillance system. The end result of this activity is to facilitate the more rapid and effective triage of patients based on information obtained across distances of miles.

Current Capabilities:

A variety of tools have been developed and tested for measurement of blood oxygen, glucose and body temperature. Sandia and Los Alamos National Laboratories have developed infrared systems for such applications (these are discussed in Chapter III (DIDA)). Thermal scans have been utilized by Canada, Taiwan, China and other Asian nations to detect individuals with elevated body temperature during the SARS outbreak in March 2003, although it remains to be seen how effective they really are in screening for disease. All the methods identified must be applicable for screening large numbers of subjects rapidly. This capability is limited compared to goals needed in this functional capability.

State of the Art:

The national laboratories have developed programs for utilizing infrared spectral analysis to determine changes in wellness of individuals. Sandia Laboratory and the private sector have developed infrared devices to enable the measurement of blood glucose and cholesterol. Infrared scanning of individuals allows for rapid determination of body temperature and was used on a large scale in monitoring which airline passengers from Asia were possibly SARS carriers during the spring of 2003. Blood oximetry allows for the determination of oxygenation of the blood; this is an important parameter in triage of patients. Miniaturization of nuclear magnetic resonance (from the Applied Physics Laboratory of Johns Hopkins University) and gas chromatography devices can now permit rapid screening of closed environments for signatures of chemical agents and precursors in exhaled air volumes. The miniature mass spectrometer device was developed from funding provided by the Defense Advanced Research Projects Agency. The Matrix Assisted Laser Desorption Ionization (MALDI), a type of mass spectrometer, has significant capabilities for identifying chemical or biological threats, but it is not available in a lightweight mobile form. Retinal scanning for diabetes is another technology allowing for rapid screening of subjects for signs of illness.

Technology Limitations and Barriers:

Among the difficulties with these rapid screening procedures is the wide range of "normal" values in the total population. It would be most useful to have a data set with internal calibrations for all persons. Alternatively, distribution curves of "normals" in each population are required if rapid screening is to prove useful. More ways need to be discovered to sense that the body (humans and animals) is giving indications of sickness. Finally, the speed with which we need to analyze the sensor feedback, in order to diagnose the individual, is technically challenging.

Gap Fillers:

Fundamental research is required on ways to discover and detect physiological clues to illness without invading the body (such as those mentioned above). (See also the Strategic Research Areas in Chapter I.) The many new non-invasive approaches to sensing physiological phenomena should be benchmarked and a study of possible synergistic combinations be performed. A library of blood component signatures (such as infrared spectrum) should be developed in support of those methods that use blood as a diagnosis medium.

MR.5 – Medical Response to Public Affairs.

The ability to manage large numbers of otherwise healthy people concerned for their well being as the result of a CBRNE event, without taxing the medical resources of the community. This management is realized through the use of public communication systems including the Internet, radio, television, the press and telephone; and by coordination with state Departments of Health, the office of the governor in each affected state and the Centers for Disease Control.

Goals:

An overall goal is providing public awareness at a sufficiently high level so that the well-informed can initiate self-help processes, thereby increasing the efficiency of medical response personnel. The specific goals identified by responders are:

- Strategy for reassurance of unaffected or minimally affected populations.
- Remote or offsite screening system which can field calls or visits (*e.g.*, reception centers, telephone hotlines, website) from potential patients who report their symptoms.
- Reduction of impact on medical resources of the affected area.
- Rapid screening for exposure to WMD agent (dealt with in MR.4).
- Capability effectiveness before people arrive at the hospital.

Current Capabilities:

At present, the strategy for reassuring the population is through non-governmental media outlets. These sources are often inconsistent. Tremendous stress is placed on medical personnel and hospital facilities as a result. Many clinical care practices (including Health Maintenance Organizations (HMOs) and Preferred Provider Organizations (PPOs) have established a filtering system between the patient and physician, sometimes called an "Advice Nurse" where providers effectively triage their clients and give medical advice via the telephone. For the larger HMOs this is a very sophisticated high-transaction-rate process. Some of the large telecommunication companies are developing call center capabilities that can handle thousands of calls an hour. This combination of technology and process would be helpful in creating this capability. A coordinated health care support center, able to handle large volumes of telephone inquiries and walk-in cases, would be necessary in the event of a biological, chemical or radiological incident.

State of the Art:

In addition to Advice Nurses and the initiatives of some of the telecommunications carriers, communities are deploying reverse 9-1-1 systems, where local emergency managers can get urgent information to their constituents via telephone.

Technology Limitations and Barriers:

This is another area where technology to enable this capability already exists. Technology to support this capability is already being pursued by commercial telecommunications companies and HMOs. The barriers are primarily policy and funding. Among the policy issues to be addressed are mechanisms to increase the numbers of lay persons who can provide assistance in a medical emergency. Under what circumstance may lay persons be utilized to provide services while liability concerns are managed? HMOs have extensive experience in managing the access to medical care providers, patients, relatives and the worried well. An examination of which procedures are most effective in increasing patient care and reducing inefficiency may improve care delivery in a crisis situation.

In the U.S. the mass communications community could provide real assistance to the public and care providers. In many cases, including the World Trade Centers in September 2001, the media served an important role. In other cases media coverage has been less than helpful, or has even hindered crisis response. Absent any serious planning media support would be uneven and haphazard at best. The federal government may want to examine the use of media to help manage a worried populace.

Gap Fillers:

There are no gap filling technology objectives recommended in this area.

MR.6 – Modeling of Exposure/Casualties for Location and Numbers. *The ability to provide automated support for understanding the likely range of exposure and casualties in particular situations, primarily the dispersal of threat agents.*

Chapter VIII (PHRBAE) discusses modeling of exposure specifically to biological agents.

The need for modeling and simulation to support responding to a terrorist incident is frequently mentioned throughout this document. Responders want to know what they are dealing with, and where. This section is concerned with modeling of radiation and chemical exposure. The desire is for a system that can not only model the dispersal of threat agents, but what the likely exposure to individuals in a given location is as the plume moves and disperses.

Goals:

The goals for this area are as follows:

- Pre-event modeling for policy and procedure development.
- Prospective, near real time dynamic modeling system for the entire U.S. in order to project future outcomes from current emerging situations (mid-event).
- Models should be able to dynamically interact with other models, databases and sensor inputs.
- Any system output must be user friendly at least at the responder command level.

Current Capabilities:

Although models exist for the effects of agents on human, animal and plant populations, none of these are real-time models; none interact with other challenge conditions (such as weather or urban canyons) and decision making tools. For example, the National Oceanic and Atmospheric Administration (NOAA) models wind movements at several hundred feet above ground level. Wind modeling below this level and in urban/rural canyons has not been demonstrated. The Department of Defense does possess real time models for agent dispersal but these are primarily for elevated altitudes. Oklahoma City has used weather radar data (Doppler) for plume modeling.

Although various federal agencies have modeled aerosol dispersal under varying conditions of wind, temperature, and surface morphologies, decision making tools based on such modern analyses are not available to emergency responders. For the most part, responders do not have any access to such modeling tools for estimating casualty level and threat dispersion during an actual incident.

Providing emergency responders with real time access to models and the capability to use such models poses a potential security risk. Such information could be exploited by terrorist if the information got to them – the majority of emergency responders are not cleared for receiving classified information. This may be a technical limitation as well as a policy issue.

State of the Art:

The Department of Defense and NOAA have developed very sophisticated modeling and simulation technology to support prediction of chemical and biological agent "plumes." Most, however, do not work in real time and little has been done to integrate the models with real-time sensor and weather information. Most of the technologists involved in this process felt that all the elements of technology needed to accomplish this functional capability are in hand and the technical risk of developing the needed capability is low.

Technology Limitations and Barriers:

There are significant technology gaps facing the emergency responder with respect to models of agent dispersal. These include determination of the dose of agent that an individual is likely to encounter if he/she is in a building (as compared to on the street). For example, what is the effect of HVAC on agent dispersal and what are the urban canyon effects? The lack of knowledge of micro-weather effects on modeling of agent dispersal is a major limitation.

The anthrax release in October 2001 revealed the differing dosage thresholds for different

populations; in one case an elderly woman in Connecticut, who received a relatively low dose of agent (presumably much less than 8,000 pfu) died from the disease. The minimal effective dose in the well population may be several magnitudes higher than that required for serious illness in the immune compromised, the aged or newborns.

The current modeling technology requires interpretation by specialists – in a crisis situation such assistance will not be readily accessible. There is no clear understanding of the level of training required for an educated responder to make effective use of real-time dynamic models. The use of modeling systems for agent dispersal and estimation of disease based on the demographic and meteorological data by the responder community may challenge the degree of fault tolerance and sensitivity of the system. A user community less aware of the limits of a model may initiate actions inconsistent with the goals of the designers of such a model.

As stated earlier, the release of dispersal models and associated information to emergency responders does have security implications as well. The cost associated with providing security checks on all emergency responders may prove to be an impediment to achieving this aim.

Gap Fillers:

The most effective approach may be teaming of emergency responders with NOAA and the private sector to develop meteorological maps that can model aerosol dispersal. A limited number of emergency responders may be trained and employed as critical regional experts in interpretation of model systems. These individuals may be vetted for security clearance and sustain a high level of readiness with appropriate compensation for this responsibility.

MR.7 – Definitive Decontamination. *The ability to remove (or neutralize) all contaminants on victims.* Although definitive decontamination is defined as the removal of all contaminants, this should be understood as the removal of contaminants to a level that is not anticipated to cause clinical signs of chemical, biological, radiological toxicity. The major aim of this effort is the dry decontamination of large numbers of persons (hundreds of persons) exposed to threat agents while they are still in or adjacent to the hot zone.

Goals:

The goals identified by the responders for this area are:

- Capability to definitively decontaminate a thousand people at a time. (Facility, personnel and supplies need to be expanded to meet the needs.)
- Tools to measure contamination in order to ensure decontamination of victim.
- Capability to do definitive decontamination of complex wounds in the field.
- Dry decontamination/neutralization system.
- A database of available and appropriate decontamination resources/processes.

The decontamination must be achieved within a time frame that assures the population does not manifest toxicity from the dispersed agents. Deployable (handheld) sensors need to be developed to measure contamination in order to ensure decontamination of victim. The technology for this is being addressed in Chapter III (DIDA). The ability to quickly expand facilities, trained personnel and supplies needs to be created. The capability must permit the definitive decontamination of complex wounds in the field. Dry decontamination/neutralization approaches should be explored (*e.g.*, UV light for some agents).[10] The purpose of the dry decontamination is to allow decontamination in very cold weather. The associated problem is that the clothes must be decontaminated, the body hair decontaminated and that this be accomplished prior to transport of affected individuals to a safe site. Responders need a database of available and

[10] Deployable trailers with heated showers, hot air dryers, and clean clothes may serve as a non-technological alternative to dry decontamination.

appropriate decontamination resources, processes and tools to assess successful decontamination. This goal is being addressed in the Chapter V (Response and Recovery).

Current Capabilities:

Several methods have demonstrated utility including the application of material with high static electrical charge; tissue paper; and the use of diatomaceous aluminum silicates. Electrostatic precipitation of biological agents suspended in air is one method to remove agent from an environment. Such techniques do not remove agent from surfaces with limited air flow (*e.g.*, nooks and crannies). Currently, removal of clothing precedes decontamination procedures for affected persons. The emergency responders believe that reluctance to disrobe in public will be a major impediment. The need to cleanse areas of abundant hair (head, armpit and groin) compounds the problem. Tools need to be developed to educate citizens and place their concerns of modesty in the larger context of physical danger. The resulting appreciation of the risk/benefit consequence of refusal of treatment may mitigate social concerns. Washing contaminated body areas with water, detergent and bleach is a preferred method but has restricted applications in cold climates. Sensors for assuring decontamination are needed.

State of the Art:

The Oak Ridge National Laboratory has a program for decontamination called REACT/S (Radiation Emergency Assistance Center/Training Site). The interagency Technical Support Working Group (TSWG) has a current broad agency announcement requesting novel concepts for rapid decontamination. Several programs exist in the United States for developing decontamination protocols for chemical or radiological agent exposure: these programs include developments by the Army's ECBC (formerly SBCCOM), and Montgomery County, MD. Technology transfer from former Soviet Union countries and Israel is being explored to achieve these goals.

Technology Limitations and Barriers:

The primary difficulty is that the nooks and crannies of the human body are very difficult to reach (*e.g.*, arm pits, body creases, groin etc.), perhaps more so with a dry material.

Contamination of respiratory airways by biological and radiological agents fosters recurring agent dispersal during respiration. Perhaps the most difficult challenge is developing rapid throughput of potentially exposed persons with sufficient decontamination to permit further movement of the population.

Gap Fillers:

The development of a dry decontamination material would be very helpful. This could be gas not harmful to humans, or a device like a lint brush with "sticky" surfaces for adhesion of agent particles. Before this can be done there is a need to develop a scientific basis for evaluating effectiveness of decontamination materials. The development of training programs for the public to appreciate the need for full body washes may be more useful in the near-term.

MR.8 – Medical Staff Surge, Re-Supply and Proper Accreditation. *The ability to identify and alert appropriate medical personnel from geographically distant areas about a CBRNE incident, and permit a rapid procedure for accreditation of professional persons that can provide assistance from distant jurisdictions.*

The technologies exist for accreditation of care givers and for establishing national databases. The distribution of individual smart cards (with date of birth, credentials, other pertinent records, biometrics, etc.) is one technological solution (See also EMPP.2 (*Mission Rehearsal, Simulation, Embedded Training and Distance Education*).) The data entered on the card will be most effective if standardized on a national level. These points and control of access to the data are therefore policy issues. The accountability of the agency for distribution of data is a major problem to be managed given recent public concern regarding large scale data assembly and acquisition.

Goals:

- Creation of a national database of credentialed individuals which could be accessed by authorized personnel, sorted, and "mobilized" when needed (*e.g.*, FEMA Disaster Assistance Employees (DAEs), medical reserve corps, etc.).
- Biometric identification.
- Database and web technology.
- Process: initial and ongoing maintenance.

Current Capabilities:

At present, individuals who wish to provide assistance during a threat situation arrive at an event without credentials. These persons could include imposters or even terrorists. Certifications are not recognized across state borders. In the Murrah Building bombing and at the World Trade Center, an appropriate deployment of the volunteers could not be realized because of the lack of certification and loss of communications. Plans for the use of skilled volunteers remain to be developed in most jurisdictions. Various regions throughout the U.S. have Disaster Medical Assistance Teams (DMAT) that are credentialed, trained, and equipped, but, there are not enough DMAT personnel to manage a catastrophic event that may occur during a WMD attack.

The Department of Homeland Security Emergency Preparedness and Response Directorate is exploring credentialing. The DoD Smart Card program is also being evaluated to determine whether it may be useful in a WMD setting.

State of the Art:

This is another area where the technology to create the capability is available. Smart card technology, along with biometrics and current Web-based information management technologies can be brought together rather easily to create this function once the policy and administrative issues are solved. These issues are also addressed in Chapter IV (UIC) and Chapter VI (EMPP).

Technology Limitations and Barriers:

This issue is not a technology issue but is rather a policy issue related to standardization of data in biometric identification, database and Web access. As such it requires evaluation of existing protocols and procedures to determine the most appropriate system for the task. The goal could be realized with little or no new technological advances. This is primarily a policy problem.

Gap Fillers:

Since the technology for accomplishing the capability exists, no new technology efforts are recommended.

MR.9 – Telemedicine in Support of Surge Requirements. *The ability to access geographically distant medical skills in real-time via telecommunications.*

It is anticipated that in responding to a CBRNE attack, there will be a need to access medical expertise that may be geographically distant from the event, either because the number of victims have overwhelmed the local medical capacity, or because the unusual nature of the injuries may require specialized expertise. The latter was the case during the release of anthrax through the postal system in October 2001.

Various scenarios have assumed that a terrorist strike with a highly contagious disease such as smallpox would lead to approximately 10,000 clinical cases within seven days of exposure. This would be the first wave. Subsequent waves would then ensue. The dissemination of an agent, if perpetrated at a major port of entry (*e.g.*, airport) would be rapid, with multiple sites immediately affected. There is no current telemedicine capability in the U.S. or elsewhere that can support medical care delivery to 10,000 patients with a highly infectious disease such as smallpox. In the event of a strike with an infectious and lethal – but not contagious – biological agent (*e.g.*, anthrax), the care of 10,000 patients would overwhelm the public health capability of the local community, but propagation of disease would not be a major concern.

A nationally distributed telemedicine capability, involving several thousand available physicians with all medical specialties, could provide access to distant care-givers. Emergency care physicians see more than eighty patients per day in emergency room environments. Under conditions of stress the processing of patients will permit fifty patients per day per physician. Under these conditions 200 physicians can manage 10,000 patients on a 24×7 basis. The use of simple dedicated telecommunications facilities, both terrestrial and satellite based, can provide a robust response to a mass casualty event. There will be minimal disruption of normal patient care in the secondary support area. This also alleviates a tremendous logistics burden and financial cost of having to transport physicians into the area of an attack.

If this sort of telemedicine capability were established, physicians and health care providers will require training familiarity with visual and auditory telemedicine devices, or several hours training, prior to a threat event.

Goals:

The goals for a telemedicine capability are:

- Haptic, auditory, and video capabilities, scalable for large numbers of casualties; multiple sites; flexible.
- Robust, encrypted (secure/protected) communications.
- Automated collection or compilation, maintenance of and access to electronic medical records.
- Ability to reach patients in their homes.
- Standardized technology protocols.
- Rapid deployability.

Current Capability:

Telemedicine is in use today for medical consultation, but has not been widely tried in the emergency/crisis context. The military has experimented with actual tele-operated remote medical procedures including surgery. In the civilian sector, telemedicine is primarily used to provide health care to persons in correctional institutions (costs of care and risk of escape are reduced).

Telemedicine capabilities are present in many regions of the U.S. including: the University of Texas Medical Branch in Galveston, the East Carolina University, and the Maryland Institute of Trauma Studies. These telemedicine programs are primarily terrestrial-based systems with a limited number of physicians at the university site. The Department of Defense Joint Medical Operations-Telemedicine program is a focus of telemedicine developments for the military.

Telemedicine practitioners at the current time do not have the experience or capability to manage simultaneously a thousand injured people. More training and exposure to telemedicine will be required. In addition, it is unclear that the medical system in the U.S. has sufficient emergency medical physicians to care for several thousand affected patients. Research is required regarding mechanisms to manage a crisis with mass casualties on the order of tens of thousands. Research is also required to understand the pool of skills available among the national public health community for such a capability.

State of the Art:

Beyond the activities described in the previous section, the DoD has completed a Telemedicine Advanced Concepts Technology Demonstration (ACTD) which advanced the state of the art in using telemedicine across great distances and in using such a system to collect data to add fidelity to the theater commanders situational awareness. The program developed and demonstrated a deployable telemedicine system that can be transported to a field of operation providing medical reach back to austere environments.

Technology Limitations and Barriers:

Current telemedicine systems were not designed to provide care for hundreds or thousands of persons. The potential throughput therefore remains to be determined. DARPA has performed some impressive work in transmitting

haptic sensation for use in telemedicine. However, the bandwidth requirements are so large it would be impractical for application to this capability in the near future. Providing robust, high-data-rate communications, that will be available even during an attack could prove challenging (see Chapter IV (UIC)).

Gap Fillers:

Research is needed into how quickly doctors and distant caregivers can screen patients via telemedicine; this research is needed so that any technical requirements can be identified that support increased throughput. In parallel a telemedicine test bed should be created that can continue to explore improvements in telemedicine to support disasters and mass casualty incidents. The telemedicine program could develop into a program for an Artificial Intelligence Virtual Clinician in the far term. The system would provide information to a caregiver on the ground in a remote site so that the patient's survival and well being is sustained. It will likely enable non-physician practitioner to screen patients. Although the subject of communications availability is critical, the government and telecommunications companies are working hard on those issues already.

Medical Response – Response Technology Objectives (MRrto)

MRrto.1 – Mass Prophylaxis Knowledge Base and Decision Aid

Objectives:

Develop a tool for emergency responder responders to use in determining the "at-risk" population in a mass chemical, biological or radiation contamination event and developing a mass prophylaxis course of action. Using data provided by available sensors, micro-weather information, demographic and medical protocol information, and other information stored before the event, the tool will provide responders with the best course of action to begin the vaccination of large numbers of victims. Taking advantage of modeling and simulation and using the information above, the tool will identify the geographic location of likely or possible victims and provide responders with a recommended course of action. The tool should include a highly intuitive Graphical User Interface (GUI) and be useable on a Personal Digital Assistant (PDA) or a laptop in a vehicle to augment the training of emergency responders. This effort should leverage and be integrated with R&Rrto.1 (*Contaminated Victim Knowledge Base*). It may be efficient to merge the two efforts.

Payoffs:

This will help emergency responders effectively identify and prepare to provide mass prophylaxis to victims and potential victims. It will help to save lives and reduce the effects of a chemical or biological attack.[11]

Challenges:

The development of such a tool is considered moderate risk. Its utility will depend on the real-time data about the event and the quality of the demographic data that can be developed about the area in question. It will also depend on the accuracy of our projections of the lethality of biological warfare (BW) agents. Recent information on the lethality of anthrax spores indicates that previous projections of the lethal dose being 10,000 spores may be off by several orders of magnitude. This may be true of other agents. Integrating meteorological information, especially in urban areas will be a challenge. Data on the susceptibility to specific threat agents may also be difficult to develop. Availability of real-time data is dependent upon the development of new and improved sensors, which are addressed in Chapter III (DIDA).

Milestones/Metrics:

FY2004: Begin research on the types of data that will be needed to be able to predict who the at-risk population is and where they are located.

[11] However, high precision will not be achieved without much greater understanding of the lethality of various agents. The ultimate level of understanding is limited not only by ethical limits on testing but by the possibility that terrorists will use a novel or modified agent for which information cannot be developed in advance.

This will likely include weather, demographics, susceptibility and threat information. Survey demographic information available in large cities and determine if that data can be used for this system. Develop strategies for acquiring the needed data. Evaluate the BW lethality information and research and assess its effect on current modeling.

FY2005: Continue research into the types of data that will be needed to accurately predict the impact of the BW event. Develop strategies for acquiring the needed data (demographic, weather, etc.). Continue evaluating research on lethality modeling. If appropriate, add funding to accelerate that research.

FY2006: Benchmark existing or emerging systems for developing course of action recommendations. Develop architectural design for the tool, collect and integrate existing information. Begin work in improving the modeling and simulation (M&S) capability using real-time data to make predictions. If possible, coordinate with R&Rrto.1 (*Contaminated Victim Knowledge Base*).

FY2007: Begin development of a prototype of the tool. Begin commercialization effort to aid in transition to responders. Continue to improve the modeling capability to support the predictive goals of the system.

FY2008: Complete development of the prototype system and begin emergency responder testing.

FY2009-2010: Continue responder testing. Deploy systems for emergency responders while continuing to integrate new products and methodologies into the system. Complete commercialization effort.

MRrto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Mass Prophylaxis Knowledge Base and Decision Aid	$9	$12	$18	$20	$20	$25	**$104**

MRrto.2 – Mass Prophylaxis Delivery System

Objectives:

Develop a tool that allows responders to significantly increase the throughput of individuals who are receiving prophylactic treatment. In cases where there are thousands of people who need to be vaccinated, one of the rate-limiting processes is the actual delivery of antibiotics, antivirals, anti nerve agents and vaccinations. Current technology such as the jet injectors used by the military can not be used for some vaccines such as ones with particulates or those that absorb alum. The objective of this RTO is to develop a system with the speed of jet injectors but with the flexibility to inject any necessary substance. The training on the system must be easy and take only a few hours. The system must be very low maintenance.

Payoffs:

This will help emergency responders protect greater numbers of people in a shorter amount of time. It will help to save lives and reduce the effects of a chemical or biological attack.

Challenges:

The development of such a tool is considered to have moderate risk. Prophylaxis media vary greatly in physical characteristics and delivery method. Injector mechanisms that can provide any kind of prophylaxis will be a challenge. The system will have to deliver a number of different drugs with very similar procedures to make training requirements as simple as possible. The clinical trials for such a system will be extensive and costly.

Milestones/Metrics:

FY2004: Begin investigating candidate prophylaxis delivery technologies and strategies.

FY2005: Award contract or grants for up to four competing approaches to developing the technology. Investigate potential applicability to everyday needs.

FY2006: Continue to fund competing approaches.

FY2007: Complete prototype development. Begin animal testing of prototype systems. Down select the best approach for clinical trials. Begin commercialization effort.

FY2008: Complete animal testing and begin Food and Drug Administration (FDA) approval process. Continue commercialization effort.

FY2009-2010: Conduct human trials. Continue testing and FDA approval process until approved.

MRrto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
Mass Prophylaxis Delivery System	$10	$30	$30	$35	$35	$50	**$190**

MRrto.3 – Casualty Management System

Objectives:

Develop a tool for emergency responders to use to manage potentially tens of thousands of victims from a mass casualty event. The systems should be able to positively track each patient either through tagging (*i.e.*, bar code) or through biometrics. The system should provide the medical/syndromic and treatment records as well as the physical location of the patient. Data should be able to be entered into the systems in several ways including voice recognition and wireless PDA keyboards. The system should be integrated with the Incident Command System to provide commanders with real-time picture of the medical operational situation. The system should be able to be used in everyday operations and scalable to be used in mass casualty situations. It must integrate with legacy systems at hospital. Finally, patient privacy needs to be ensured in the design of the system. The work should be managed in tandem with that of EMPPrto.3.

Payoffs:

This will help emergency responders effectively manage very large numbers of victims. It will reduce mistakes in treatment, provide important information for incident command and even prevent losing patients amidst the chaos of a catastrophic event. It will help to save lives and allow the medical community to treat the casualties more effectively.

Challenges:

Voice recognition in noisy environments is very difficult. This capability must be highly reliable because it will be the method for entering patient data into the system, and that increases the challenge. Integration with legacy systems is always a technical challenge. Interoperability with command systems may prove difficult. The ability to support hundreds of practitioners in the field, all at once and wirelessly, may present bandwidth problems.

Milestones/Metrics:

FY2004: Benchmark systems that track objects through processes such as that used by parcel delivery services. Evaluate current patient management systems especially those intended to manage thousands of patients like the Defense of Department. Evaluate the state of biometric identification and other ways to positively identify and track patients. Determine the available enabling technologies and begin development of a Casualty Management System Architecture.

FY2005: Continue to develop the system architecture. Begin first prototype system development with available technology even if it falls short of goals but improves capabilities. Begin commercialization effort.

FY2006: Complete system prototype and begin field testing the system in realistic situation where thousands of victims must be processed. Adjust system design based on result of testing and review opportunities for technology insertion to increase capability.

FY2007: Continue field testing. Begin development of second prototype. The second prototype should be able to handle ten thousand patients in 24 hours. Complete commercialization efforts. Transition initial capability for use by responders.

FY2008: Complete development of second prototype. Field test second prototype. Transition improved capability to responders through commercialization efforts.

MRrto.3 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Casualty Management System	$2	$3	$4	$7	$6	**$22**

MRrto.4 – Telemedicine Testbed

Objectives:

There are three objectives in this RTO. First, establish a telemedicine testbed where research on new concepts of operation and new enabling technology can be explored to support disasters and mass casualty incidents. Second, conduct research on how quickly doctors can screen patients via telemedicine. Third, develop an artificial intelligence virtual clinician, with the ability to provide medical advice to a distant practitioner without a physician being directly involved.

Payoffs:

This will help responders screen and treat more victims in a shorter period of time. It will allow reach back to specialists who may not be in the area of the incident. It could provide access to doctors or credible medical advice to an incident anywhere in the country. This could also provide an important capability to health care in remote areas on a daily basis.

Challenges:

The biggest challenges will be creating the telecommunications and information technology capacity necessary to bring access to hundreds of doctors to an incident, training enough clinicians to test the system, and of course the long-term research into building a virtual clinician.

Milestones/Metrics:

FY2004: Begin development of a telemedicine architecture for the testbed. Issue a broad area announcement for a health care and research organization to host the testbed and begin research on how quickly physicians can screen patients using telemedicine.

FY2005: Continue research on how quickly patients can be screened and begin work on bringing large numbers of physicians on line to respond to a mass casualty incident. Begin work on a virtual clinician capability.

FY2006: Continue optimizing the telemedicine capability. Test the system in mock disaster exercises. The goal is to screen at this point is to screen at least 5,000 patients in 24 hours. Continue work on virtual clinician.

FY2007: Begin investigating strategies for deploying a robust telemedicine capability around the country. Investigate how to host the disaster telemedicine system on existing or easily modified infrastructure. Continue testing and exercising the telemedicine system. Continue add capability and use the system including virtual clinician capability, if available.

FY2008: Continue to test new capability and respond to disasters. The goal at this point is to screen at least 10,000 patients in 24 hours. Integrate new virtual clinician capability. Deploy systems in other cities as funding allows.

MRrto.4 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Telemedicine Test Bed	$5	$10	$12	$15	$10	**$52**

MRrto.5 – Novel Decontamination – Research

Objectives:

This will help responders effectively decontaminate large number of victims in the event of a chemical or biological attack, especially in cold weather. It should significantly increase the throughput of people being decontaminated and

will probably save lives. This is fundamental research, which should focus on use of gaseous material (benign to humans but not to threat agents), ultraviolet light and other energy sources, and powders and kinetic methods.

Payoffs:

Responders would prefer a capability to decontaminate people without liquid or soaking decontamination materials. The decontamination method should be able to quickly reduce the threat to levels that do not cause toxicity, in all weather conditions, without the victim having to remove all their clothes. There are currently no known dry materials that can decontaminate a range of agents but are also benign to humans.

Challenges:

There are currently no known dry or gaseous materials that can decontaminate a range of agents that are also benign to humans.

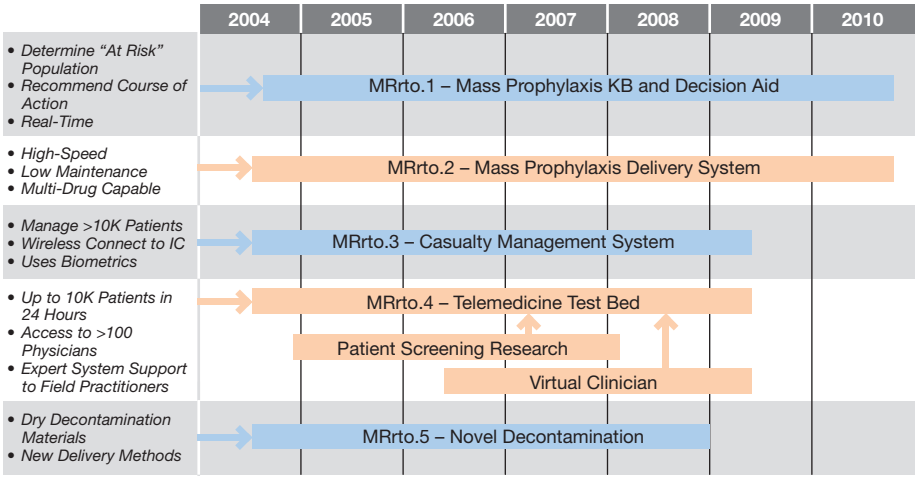
Milestones/Metrics:

FY2004: Begin research into various materials and strategies for dry decontamination of people. Issue a BAA seeking new ideas to accomplish the goals set forth above; award several significant grants to research activities to fund several approaches. This is fundamental work and will need to be continued until breakthroughs occur or the science community runs out of credible ideas to pursue.

FY2005-2008: Continue fundamental research into various approaches for dry decontamination. By 2006 or 2007 it may be possible to begin some applied research.

MRrto.5 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Novel Decontamination	$2	$4	$6	$6	$6	**$24**



Medical Response Technology Roadmap

Chapter VIII

Public Health Readiness for Biological Agent Events (PHRBAE)

Chapter Chair: Dr. Stephen Kornguth
Chapter Coordinator: Michelle Royal

Definition

Public Health Readiness for Biological Agent Events (PHRBAE) is the capability for public health infrastructure and health care delivery systems to be prepared for and respond to an event involving biological agents.

Biological agents include bacteria, viruses, fungi and biological toxins. While biological toxins are essentially poisons of biological origin, the first three are infectious, meaning that because they can multiply in the human body, a very small amount of agent can cause illness. The most serious biological attacks may involve a subset of the infectious agents that are especially contagious – disease is easily communicated from person to person, raising the possibility of epidemic or even pandemic spread. As the recent SARS epidemic demonstrated, the medical system channels sick people into the care of health professionals, meaning that an especially virulent disease organism will be automatically vectored against those assets that are needed to contain and treat the outbreak.

This NTRO is not a complete recipe for readiness to deal with a biological attack. First, the overall scope of Project Responder has excluded innovations in medical treatment such as improved vaccines, antibacterials, and antivirals. Second, many key elements of preparedness, such as networked sensor systems for detection of an urban airborne biological agent release, are included in other NTROs where they have commonalities with preparedness for chemical, radiological, nuclear, or explosive and incendiary attacks.

Operational Environments

This NTRO is only concerned with biological agents, so the other (CRNE) attack modes are not relevant. Within biological agent incidents, it is possible to distinguish among different sorts of attack. There are three major categories of biological threat agents: highly infectious/contagious organisms that will replicate in a human or animal host and generate new infectious bacteria or viruses (*e.g.*, smallpox, ebola); live organisms that will cause disease in a host following exposure of the host but that are not readily transmitted from one person to another (*e.g.*, anthrax); and biological materials that can cause severe clinical distress or death in a human or animal but do not have the ability to replicate (toxins). Although materials from all three categories can cause illness, the virulence of the first one and the possibility of pandemic makes it of special concern. The distinct modes of exposure and course of illness characteristic of different agents means that the type of agent is indeed an important factor in determining the appropriate response. However, using the type of agent to distinguish among operational environments makes only limited sense because often the type of agent involved is something that only becomes clear over the course of an incident.

Instead, progression of exposure and disease provides the defining characteristic for the operational environments. A successful biological attack is likely to be mounted covertly, with the dispersal of agent going unnoticed. Without widespread deployment of advanced technology sensors (see Chapter III (DIDA)), sick patients

appearing in doctors' offices and emergency rooms will likely be the first indication that anything is awry. Thus the first and primary responders in this event may be health professionals rather than the public safety officers who are typically the responders in the other NTROs. There are major differences between technologies that are important before symptoms are widespread, and technologies that are useful after mass illness has occurred. In the case of contagious disease, exposed victims may present a continued threat to others, extending the attack in time and geography. Therefore, the operational environments associated with the PHRBAE NTRO are: Pre-Event, Immediate Post-Dispersal, Initial Post-Symptomatic, Mass Illness, and Recovery.

The use of biological agents by hostile nations or terrorist groups differs from other WMD threats. This is because the clinical signs resulting from exposure to biological agents may take 48 or more hours to emerge and because the replicating nature of all the biological agents (except toxins) causes a persistent clinical threat well after the first episode has completed its course. While not a focus of the NTRO, it is also worth noting that the improved capabilities it would afford would also be relevant to naturally occurring emergent diseases. With the exception of the anthrax release through the mail in October and November 2001 and the Salmonella poisoning event of a decade ago in Oregon, all disease outbreaks in the continental United States were naturally emergent diseases. This is generally true on a global scale. Therefore steps taken to ameliorate the clinical impact of biological agent attack will generally improve the health of all U.S. citizens and residents and have beneficial consequences for medical care world-wide.

Needed Functional Capabilities and Priorities

In order of declining priority, the needed capabilities for PHRBAE are:

- Surveillance & Information Integration Systems
- Rapid, High-Throughput Clinical Assessment and Testing
- Modeling of Exposure and Containment
- Isolation and Quarantine
- Affordable Specimen Transport for CW/BW Agents
- Transport of Contagious Patients
- Safe Handling of Medical Waste

The functional capabilities are presented in priority order based on responders' input in workshops and field interviews conducted during the earlier phases of this effort and subsequently modified or validated in both responder and technical workshops in this phase.

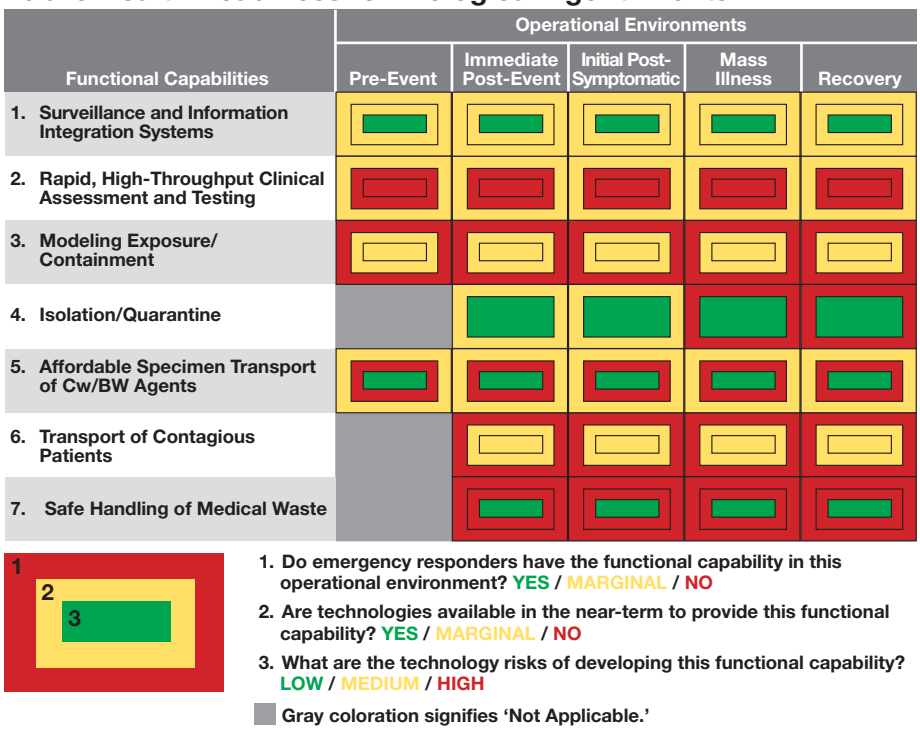
Surveillance and Information Integration Systems (PHRBAE.1) was universally assessed to be a high priority and this was also ranked as the most important functional capability to fulfill. *Rapid, High-Throughput Clinical Assessment and Testing,* (PHRBAE.2) and *Modeling Exposure/Containment* (PHRBAE.3) also received a large number of high-priority votes from the responders. *Isolation and Quarantine* (PHRBAE.4) received a wide range of rankings, from high- to low-priority. The functional capabilities of *Affordable Specimen Transport* (PHRBAE.5), *Transport of Contagious Patients* (PHRBAE.6), and *Safe Handling of Medical Waste* (PHRBAE.7) received only mid- and low-level priority rankings.

Overall State of Technology for Public Health Readiness for Biological Agent Events

The matrix on the next page shows a wide variety in the readiness of technology to meet the needs of responding to biological agent event.

Several of these capabilities require new technological developments (*e.g.*, the identification of biomarkers for human exposure to biological threat agents) while others require acquisition of costly equipment (*e.g.*, transport of infected patients) or a thoughtful restructuring of current

Public Health Readiness for Biological Agent Events



administrative policy (*e.g.*, development of command and control infrastructure and procedures for quarantine). In other important areas, such as surveillance, the needed technology is well in hand and merely needs to be applied in a standardized framework.

PHRBAE.1 – Surveillance and Information Integration Systems. *The capability to do routine near-real-time processing of epidemiological and veterinary data to provide early detection, identification, assessment, and tracking of exposure to biological agents.*

Since early appropriate prophylaxis and treatment can often dramatically improve health outcomes, early alerting of an attack is crucial. In the absence of physical discovery of the attack itself, the first indication of an attack will be sickened people and animals. Data sources for alerting information may include hospitals, emergency rooms, ambulance and other EMS services, clinics, doctors offices, schools, pharmacies, veterinarians, coroners, laboratories, nursing homes, major employers (including military installations), prisons, and points of entry into the continental U.S. (CONUS) for humans and livestock.

The surveillance system should include both automated reporting of data for routine analysis and collation of reports by health professionals of unusual cases and patterns.

Early detection has three components: data input, data analysis, and display of information. The data input includes archival data sets, current and emergent disease-related data sets, and reports from primary emergency medical care. Effective response decision-making requires (1) access in real-time to the full spectrum of health related data (archival data sets with seasonal patterns of disease incidence and prescription and over-the-counter pharmaceutical demand, current status-of-patient reports) throughout a network; (2) the ability to evaluate and disseminate specific actions and resource allocation requirements (including focused epidemiological and clinical investigation) following integration of the information; and (3) capability to transfer data electronically to alternative decision makers when situations such as task overload occurs.

Archival data sets for occurrence of disease in the U.S., during the past three years are available through most of the state departments of health. Diseases and symptoms requiring public health reporting can be tracked through the Center for Disease Control (CDC). The incidence of illnesses not subject to reporting requirements is more difficult to characterize. Today, statistics on emergency room visits across many hospitals could provide an understanding of disease emergence but only with a significant delay after the disease presents clinically. Physicians use codes from the International Classification of Diseases,

ninth edition (ICD-9) to define the illnesses (and cause of death) of patients; assignment and reporting of the ICD-9 codes now lags presentation of clinical signs by 24-48 hours or more—somewhat late for dealing with the initial cases of fast-onset infections. Moreover, novel or rare diseases are likely to be mischaracterized at the start, further delaying clear reporting.

The initial recognition and description of an emergent illness greatly eases the identification of subsequent cases of illness (*e.g.*, anthrax in October 2001, SARS and monkeypox). Once an illness is identified and either its signs and symptoms codified or a clinical test developed, it can be readily tracked. However the concurrent emergence of two or more biological diseases or a similar disease with two or more sources of agent greatly increases difficulty in diagnosis and tracking, and this possibility must be taken into account in preparedness and technology development.

Prior to diagnosis and the assignment of an ICD-9 code, illness may be classified by presenting signs (syndromic characterization) and most emergency room admissions nurses – and, increasingly ambulance and other emergency medical service (EMS) personnel—do categorize the patient in this way.

A large number of patients in a reporting universe may be needed to detect initial disease outbreak merely on the basis of statistics; a small but geographically dispersed initial outbreak (such as might result from exposure in a hub airport or even a metropolitan train station) would be especially difficult to identify unless travel information were routinely included in reporting.

Goals:

A primary goal is the near-real-time capture (ideally within six hours of early clinical signs) of indicators that a disease with high threat potential is emerging in a community. To enable capture of such data, an automated data collection and retrieval system is necessary and the reporting of this data should be mandated on a national level with associated funding to support this activity. The acquired data must be compliant with health privacy regulations (HIPAA) and transmitted to the appropriate users with secure communication systems.

This will by necessity be an evolutionary system because few of our medical facilities utilize real time electronic admission protocols or systems; therefore the adopted process should integrate (to the greatest extent possible) the output of legacy systems while encouraging hospitals, clinics, and other reporting entities to move toward systems that immediately capture interactions in digital form.

The acquired information at the local level must be integrated with regional and national data because of the highly mobile culture in which we live.

The presentation of the data should include both geographic and time dimensions. It should be iconographic and scalable to permit comprehension by the user community that an event is in progress. The software must also provide multiple views to allow analysis of the data; for example the geographic and temporal data should be able to be overlaid with actual weather and wind data, local and regional transportation systems, and commuting and other movement patterns. The system should automatically provide all the information and contacts needed for more detailed epidemiological investigation (identification of index cases, etc.). The system must be user-friendly to public health experts and epidemiologists. The tactical decision making under stress (TADMUS) program developed by the three military departments can serve as a model for this activity.

In addition to these advanced data displays, the systems should include validated, highly credible, probabilistic models for analysis of the data. This would permit detection and assessment of deviation from baseline rates based on archival data as adjusted for seasonal, weekly, and other variation and demographic change.

Advances in rapid clinical assessment and testing, including the sensing of specific biomarkers of

infection as described in PHRBAE.2 (*Rapid, High-Throughput Clinical Assessment and Testing*), would be highly complementary with the surveillance system. The surveillance system indicating unusual numbers of cases could prompt the use of tests that might not otherwise be ordered, and affordable and rapid clinical screening would increase the specificity and accuracy of initial diagnosis and thus increase the power of the surveillance system. Even rapid tests that are not capable of identifying biological warfare agents but that commonly result in earlier diagnoses that exclude biological warfare agents as the cause would improve the power and speed of the surveillance system by reducing the background noise against which a biological agent event would need to be detected.

Similarly, the widespread deployment of networked environmental sensors capable of detecting airborne biological agent (DIDA.5 (*Detector Arrays and Networks*)) and improved surveillance of the food chain for foodborne pathogens (MRPA.1 (*Rapid Diagnostics and Detection to Confirm the Introduction of CBR Agents to Animals, Plants, and Food/Feed*)) would also be highly complementary with the epidemiological surveillance capability. The surveillance information display should also easily interoperate with programs for collecting weather information (DIDA.7 (*Collection and Dissemination of Weather and Environmental Conditions*)) modeling agent dispersal (DIDA.6 (*CBRNE Effects Modeling and Simulation*)), exposure (MR.6 (*Modeling of Exposure/Casualties for Locations and Numbers*)), and onward contagion (PHRBAE.3 (*Modeling of Exposure and Containment*)). Finally, the EMS and healthcare aspects should be integrated with the health resource optimization and casualty management data systems in other NTROs (MR.2 (*Mass Casualty Medical Care Management*)) and EMPP.4 (*Alternate/ Mobile Hospital Contingencies*)).

Because the likelihood of a WMD event is low, even as the consequences can be catastrophic, training of response officials in the use of the system should require less than four hours. The developed system should include automated decision support tools; analysis tools and the output must be a simple product-with no requirement for local technical support.

Current Capabilities:

Many metropolitan public safety agencies have established multi-source reporting systems but without the scope, reporting rapidity and frequency, regional and national integration, detail or analytic power envisioned under this functional capability. Summary information on 9-1-1 and EMS calls are already generally available to public health departments but not always with the timeliness, analysis, and level of detail that would make them fully useful. They are not typically summarized in a standard manner, and are often not collated across jurisdictional lines.

New York City has a syndromic surveillance system in place that is widely regarded as one of the best. Many modern hospitals have adopted electronic data entry of syndromic signs because this facilitates billing procedures and cost recovery; several systems have been prepared by the private sector (*e.g.*, Cerner and Eclipsys) for this purpose. Such data can be made available for surveillance in real time. Privacy rights of the patient are a primary concern, but all personal identifiers in the data may be removed prior to screening by public health and emergency response officials. Reportable data (*i.e.*, data on illness required to be reported to public health authorities) is examined for significant increases (compared to normal expectations based on seasonal and weekly patterns, and local weather and other sources of variation) in illness having particular clinical manifestations (*e.g.*, rash, bleeding from orifices) as well as less specific indications (respiratory distress, fever).

Several nationally funded programs have explored methods to identify emergent disease from hospital admissions and have met with limited operational success. One major difficulty is that health care providers have limited time for processing the additional paperwork that most of these systems require today. Clinics, free standing urgent care facilities, and doctors' offices may be even richer sources of early indications of an outbreak, but these are even more decentralized than hospitals, and so a major effort would be

needed to attain adequate participation. The data to be captured must benefit the hospital administration, physician or allied health person in a cost-effective manner. While the primary driver of the electronic data entry system may be early recovery of payment from third party agencies such as Blue Cross/Blue Shield, advocates of fully digital case management (including links to the pharmacy and automated filling of prescriptions and tracking of clinical tests and their results) suggest that it can reduce medical and pharmacy errors and cut costs as well.

An additional parameter that has been considered for early indication of emergent disease is purchase of over-the-counter pharmaceuticals or health care items (*e.g.*, analgesics, antipyretics, tissues for the nose). Many of these items are effectively stockpiled in the home and purchased as part of periodic shopping trips (*e.g.*, on weekends, coincident with grocery sales); therefore these data may not provide sensitive early indication of emergent disease. Proprietary issues include the reluctance of stores to reveal information that would compromise a competitive edge. Private hospitals are also reluctant to provide daily occupancy information to competitors because of the proprietary nature of the information. Trust building is thus a major concern.

Once archival data sets have been established and real time syndromic data are obtained and processed, a variety of statistical techniques can be used to assess the significance of apparent deviations from the baseline. Appropriate software, together with expert judgment, could suggest a full-blown alert or a call for more detailed clinical and epidemiological investigation.

In the current environment, near-real time, fine-grained electronic surveillance in medical facilities is not available, although some communities have developed data reporting and alerting procedures based on grosser indications. Few localities have automated download capabilities to public health servers. At present, approximately 15% of emergency room facilities capture data digitally and so could be used to track emergent disease.

Archival data sets currently exist for disease incidence in most states in the U.S. and for much of the developed world. Data relevant to emergent diseases may also be obtained from the World and Pan-American Health Organizations and other relevant international agencies. However, what one really wants for a baseline is data collected in the same way and format as the data being collected on a current basis. Thus a syndromic surveillance system will only be maximally effective once it is in place long enough for a baseline of syndromic data (and not just finished diagnoses at a later stage of disease) to be able for comparison. The increased geographical distribution of West Nile Virus during the past three years has increased vigilance and monitoring of diseases in birds. The West Nile Virus outbreak was first recognized because of the large number of deaths of birds in the New York area (and particularly at the Bronx Zoo). As a result of the lessons-learned analyses from that event, state health laboratories, regional zoological societies and federal laboratories have developed communications linkages and network programs and have resurrected decades-old efforts to maintain and watch chickens as disease sentinels for bird-borne illness.

State of the Art:

The information processing technologies required are not different in kind from those in use by large commercial enterprises (for example, Wal-Mart) to track, analyze, predict, and respond to various components of consumer demand on a near-real-time basis. Nearly every capability imagined has been demonstrated in one research project or another. However the heterogeneity of data sources, the multiplicity of regional users, the concern for privacy, and the need for early response to and focus on small signals in the data imposes additional challenges. Thus the required technology integration will not be entirely straightforward.

Project Responder has identified at least nine local, regional, and national efforts to standardize data formats and provide timely information. Many of these are Web-based and provide hospital, EMS, and/or pharmacy status to users and

can issue a web alert and/or alert emergency room doctors and public health specialists via pagers. Some provide both spatial and temporal displays of the surveillance data and statistical analysis of the data compared to expectations.

The National Electronic Disease Surveillance System (NEDSS) is an initiative of the Centers for Disease Control that promotes the use of data and information system standards to advance the development of efficient, integrated, and interoperable surveillance systems at federal, state and local levels. CDC's Health Alert Network (HAN) is developing Internet connectivity at state and local health departments; this mechanism could be used for exchanging information and for distributing alerts based on surveillance.

ESSENCE II (Electronic Surveillance System for the Early Notification of Community Based Epidemics) is an operational prototype testbed for the National Capital Region being used to test concepts and technologies that are not mature enough to be fielded by local health departments. Sponsored by DoD, ESSENCE II is integrating military and civilian health indicator data, evaluating non-traditional data sources, and developing new analytical techniques to identify abnormal health conditions.

Commercial systems enable capture of syndromic data or confirmed diagnoses in health care facilities. Although there is currently no standardization of approaches across these multiple systems, the CDC is developing standards for syndromic surveillance. Large national programs are developing technology to identify biological agents in livestock, to encourage the use of sentinel chickens and establishment of joint efforts between zoos and state departments of health (see MRPA.2 (*Coordination of Animal and Plant Entities with Public Health, Law Enforcement, and State, Local, and Federal Government and Industry*)). DARPA has funded the Bio-event Advanced Leading Indicator Recognition (BioALIRT) project for advanced surveillance techniques and the ENCOMPASS Project to demonstrate techniques for effective allocation of resources when a crisis situation has emerged.

In 2003 the real time acquisition and transmittal of electronic data from large hospitals and other health system participants is technically feasible. There is a need to identify baseline standards for machine data analysis and presentation in an iconographic format that is comprehensible. The integration of different agencies, communities and disciplines (to include veterinary) into the surveillance effort is technically feasible. The overlay with transportation lines, water systems, commuting patterns, weather data, and the like is not technically difficult but it may be costly. The automated alerting function, even once made reliable, should still be backstopped by the flexible display of all the data and the ability for experts to manipulate the data for appropriate display. (This is needed for detailed investigation in any event.)

Technology Limitations and Barriers:

As implied in the previous discussion, the major barriers are institutional rather than technological, although integration of disparate software systems can pose thorny problems. Privacy issues are of some concern as well, although there is clear precedent for reporting based on public health needs.

Business incentives lead to reluctance on the part of pharmacies and health providers to participate prior to the confirmed outbreak of a disease. There is a need for trusted agents who will interface between public health and emergency response agencies, pharmacies and medical centers as an integrated system is being created. Some technology is required to allow for automated data input, regional monitoring of data and the reduction of background noise until a large enough data set is established.

Because there are thousands of emergency rooms and many more doctors' offices, data acquisition will be costly and cumbersome unless it is built into the medical reimbursement system. Detailed information of causes of death is not reported on a timely basis in many medical examiners' offices because of cost and low numbers of autopsies. There is a requirement for research to determine what types of information should be

collected (and to what level of detail) and the cost effectiveness of such information.

Gap Fillers:

Perhaps the most immediately available and most sensitive early indicator of severe acute illness is 9-1-1 call and EMS treatment records. These are largely accessible to public safety departments now, and efforts at standardization of data are underway. This is probably the "lowest hanging fruit" for immediate improvement in capability. Multiple projects are already under way to collect such data. What is needed is a forum for demonstration of what is being done and harmonization of the different approaches and a path toward full interoperability in the future.

For many threat agents, the onset of severe illness is too late. Picking up indications of less severe initial symptoms is a harder problem – clusters of work absences may be the earliest indicator and detailed reporting from doctors' offices and clinics may be the best indicator. Despite the difficulties, several of the regional demonstrations have shown promise in improving the early recognition of disease outbreaks. Further research and analysis is needed to understand the relative cost and value of including various sources of information in the surveillance system. Such understanding is needed to guide the evolution of the overall surveillance system. A key factor in such value-of-information approaches is the cascade of actions that follows from a warning being delivered. Such actions include further investigation of the possibly identified outbreak as well as moves toward containment and treatment.

For the overall surveillance system to be maximally effective, interoperability of data sets and data standardization is needed to facilitate robust data mining. Data mining and statistical comparison of actual data with expected rates (based on history, seasonal and weekly patterns, etc.) is the key to early detection of disease outbreak. Thus an important initiative will be harmonization of data standards.

In all of these examples many existing programs are pointed in the right direction. Systems integration is the biggest technical challenge, with the technical challenge itself being dwarfed by the difficulties in getting private sector organizations to cooperate and the need to assure that privacy requirements are adhered to.

PHRBAE.2 – Rapid High-Throughput Clinical Assessment and Testing. *The capability to do rapid testing of clinical specimens to determine the nature of an infectious agent so that specific treatment can begin before the appearance of symptoms.*

Rapid clinical assessment and testing is important because of the dramatically improved health outcomes that can result from early treatment and isolation of affected individuals. The capability is applicable to biological agent events in three main contexts: screening of large numbers of possibly exposed individuals who have been in the vicinity of a suspected biological agent release to see if they are likely to become ill; containing the spread of an epidemic by determining if individuals are infected and contagious, ideally recognizing initial human spreaders of disease and certainly rendering isolation and quarantine more efficient; and identifying the pathogen in a patient so that specific treatment can begin as soon as possible and ideally before appearance of severe symptoms.

The three contexts impose somewhat different requirements but some common technologies are useful across more than one. Some tests may look directly for the offending organisms; others look for an early systemic response (for example, stress factor or antibody production). Different types of agents and agent-induced illness will be more or less susceptible to detection and identification by these different methods, and this susceptibility will typically be different at different points over the course of an illness induced by biological agent. Shortly after initial exposure, an agent may be detectable in the mucosa or on the skin, but very sensitive detection would be required for this type of detection to succeed against organisms that can cause infection even in very small numbers. Some time after that, but still before the onset of clinical symptoms, it may be possible to detect systemic responses. During this phase it may be still be hard to detect the

infectious organism itself in the body. The systemic response may be detectable long after the illness has past and the patient is no longer contagious, producing a false positive if the test is intended to be used for an index of potential morbidity and contagion.

For these reasons, as well as the wide variation in healthy physiology, there is unlikely to be one test or set of tests that can be used in all contexts for all suspected pathogens. In many cases the best solution is a fairly imprecise screening test followed by a more exact (and probably less rapid) test where the screening test raises concern.

As noted previously, routine use of such testing in emergency rooms, urgent care clinics, and doctors' offices would significantly improve the power of the surveillance system discussed in PHRBAE.1 (*Surveillance and Information Integration Systems*). If, as is likely, the capability also identifies normal disease agents more rapidly than current medical practice, then its adoption in routine medical care would also produce a general improvement in health. (Health would be further protected through a dramatic reduction in the inappropriate use of antibiotics, leading to reduced proliferation of resistant bacteria.)

Goals:

A primary goal is the rapid detection and identification of multiple threat agents in biological samples from human and animal sources. Responders would like a system that rapidly and accurately assesses a patient for all possible illnesses without invasive sample taking, at low cost, and ideally without any previous information on the nature of exposure. Traditionally, most medical tests are deployed to screen for particular conditions or to rule out particular diagnoses rather than to determine health and exposure status to all harmful organisms, so this goal amounts to a revolution in screening and diagnostic practice. Such testing would be maximally effective in initial detection of an attack on the general population if it were incorporated in everyday medical practice in doctors' offices and clinics, as well as emergency rooms and hospitals. This would be likely to occur because a technology capable of performing the desired detection and characterization of infection with threat agents would likely also be able to diagnose naturally-occurring infections.

In each of these settings identified above, a key goal would be for the test to be rapid enough to allow a single encounter with the individual being tested so the sample or signature can be acquired, the test run, and the results made available before the individual leaves the controlled setting of the test venue. Otherwise the individuals must be called back with results and there is an inevitable leakage of patients from the system and a lag before treatment or other appropriate intervention can be started. If a single encounter is not practical, then an important element of the overall system would be record keeping and possibly biometric identification to ensure that individuals can be contacted and that identity information is maintained through the process.

Responders indicated that ideally the sampling system should be field deployable, non-invasive and be completed in less than a minute. The most probable system concepts would involve multi-level screening. The first level would indicate presence or absence of threat agent while the second would verify the initial positive reading and identify the agent. Clearly a very low rate of false negatives is essential in the first level of screening. Training for responder use of the screening system should require less than 1 hour and therefore the methodology must be transparent.

In our workshops, responders imagined a release of biological agent in a stadium; they would like to be able to screen all attendees on the way out—requiring total processing times per person of a minute or so at most. The most preferred situation would have infected individuals readily identified by some spectral image within sixty seconds from a distance of greater than ten feet, or by breathing into an advanced breathalyzer. This is not achievable currently. An intermediate solution would utilize sweat and nasal swabs, or small samples of blood (<10 microliters) taken for example by a capillary prick. The time

required for obtaining these samples would approximate thirty seconds leaving a minute at most for processing to meet the responders' ideal throughput requirement. In this case a screening test for exposure could be supplemented by a more detailed test to identify the agent. Obviously in this scenario the supplementary test to characterize the agent need only be given to a small subset of exposed individuals—to identify the agent and to ensure that only one agent had been dispersed.

However, for ill patients in an emergency room or hospital, even tests that took an hour or more would be substantial improvements over standard differential diagnosis techniques and would meet the single encounter standard.

Current Capabilities:

Current capabilities are limited to traditional medical diagnosis tools in the hands of trained medical personnel.

State of the Art:

Current technologies permit thermal imaging of individuals to determine if they are febrile; this technique has been employed during the SARS epidemic to screen persons traveling from the hot zone (China, Hong Kong, Taiwan) to the U.S. However there is no experimental data assuring the value of this approach.

In hospital environments, it is now possible to identify many threat agents using genomic (DNA/RNA) or proteomic (antibody) based tests. Some genomic systems are deployable and weigh less than forty pounds (*e.g.*, Cepheid). These systems allow detection of a limited number of threat agents or sequences, but systems that allow greater parallelism are emerging from the laboratory (Nanogen, Sequenom, Applied Biosystems). The proteomic systems can be adapted to paper strips similar to that for blood glucose monitoring by diabetic, or adapted for smaller sample sizes through automated fluorescent readout (Rules-Based Medicine). The proteomic systems are subject to cross-reactions and therefore have a significant false positive rate.

Transdermal IR spectroscopy can reveal the presence of low molecular weight metabolites in blood and this may provide indication of chemical (*e.g.*, nerve agents) or biological agents (toxins) that markedly reduce blood glucose, oxygen or other vital materials. This technology complements iontophoresis (electrically-driven transport of small molecules through the skin) that is used commercially in the GlucoWatch, a wrist device diabetics can wear, to monitor their blood glucose profiles.[12]

The recently completed human genome project has permitted researchers to identify early biomarkers of human response to threat agents. This technology, funded in large part by the Department of Health and Human Services (HHS) will allow rapid growth in this general arena.

Novel research tools, based on human genome expression, are correlating the appearance of inducible protein with various disease states. Research to this point suggests that such host response biomarkers may permit clinical investigators to determine whether an individual has been exposed to a pathogenic agent. Such changes may appear within 4-10 hours following exposure. Various corporate entities have developed platforms for rapid screening of inducible proteins that may have utility as biomarkers of exposure and disease (*e.g.*, Affymetrix, Roche, Chiron, Rules-Based Medicine, Biosite). Even if the biomarkers can only differentiate bacterial from viral agent exposure, treatment and prophylaxis may be initiated while the individuals are pre-symptomatic. It would be useful to develop software that correlates syndromic surveillance and biomarker expression patterns.

Technology Limitations and Barriers:

There is no current technology available for the non-invasive rapid characterization of biological

[12] However the GlucoWatch is marketed only as a supplement and not a replacement for regular blood glucose metering. It must be calibrated each time it is worn and it is far from instantaneous—it takes 2 hours to "warm up" and then produces readings that are time-averaged over twenty minutes. So a capillary prick is much faster and more accurate.

agents in the body including viruses, bacteria, fungi and toxins. Characterizing biological agents in clinical samples is also problematic. Point detectors are currently available but require significant time and their ability to detect small amounts of agent in biological samples such as mucous is not clear. Genomic analyses require a sample preparation of approximately ten minutes to release the DNA or RNA. Subsequent processing is also on the order of ten or more minutes. Genomic analyses, if done with sufficient well-identified and appropriate probes will be very accurate with very few false positives or negatives. Proteomic analyses based on immunological reactions will require much less time (approximately five to ten minutes) but cross reactions between the immunoglobulin and related but non-pathogenic organisms will result in significant false positives and negatives. While genetic engineering of threat agents can circumvent the immunoassay-based systems, appropriate genomic probes should be able to detect the organism anyway.

The genomic systems can utilize samples in the tens of microliters (drops) because of nucleic acid amplification. Proteomic analyses may require somewhat larger sample volumes. Several identified proteins that are induced following infection are also induced by stress not related to infection (*e.g.*, pregnancy) and so are not reliable indicators.

DARPA is developing a single, hand held device that is anticipated to use proteomic and genomic technology to detect infectious agents. Microelectronic chips that can detect biological threat agents are under development in the commercial sector as well. A Nanogen on-chips strand displacement amplification technique and third wave technology invader systems are non-polymerase chain reaction systems. The feasibility of detecting biological agents in the field by these methods remains to be demonstrated. These will have a rapid-turnaround if successful.

At the present time there are no truly non-invasive rapid analytical systems for detecting threat agents or host response markers for infection. Transdermal detection of blood metabolites is most effective for low molecular weight materials (not proteins). However, IR spectroscopy is so far unproven and iontophoresis is slow.

Electronic nose technology developed at several universities, including The University of Texas at Austin, Department of Energy National Laboratories and private industry may provide tools with utility but this is an emergent technology. The idea is to sample the breath or perhaps sweat and/or saliva.

Gap Fillers:

The disease process for threat agents – including the body's response—is imperfectly understood. An effort to learn more about the biomarkers that correlate with different stages of the disease process for different biological threat agents has been proposed as a Strategic Research Area (see Chapter I (Introduction)).

The panoply of technical approaches to rapid clinical assessment and testing must be winnowed over time to the level of a few alternatives for serious investment throughout the medical community.

However, responder interest in an extremely rapid test that can be administered if necessary without trained medical personnel suggests an early emphasis on evaluating the power of transdermal IR chromoscopy to detect low-molecular weight biomarkers. If this approach pans out, then the development of a library of infrared spectral properties of blood components, which can be used to determine the presence of biological agents, will benefit both responders dealing with chemical and biological threats as well as the general medical community.

To the extent that the testing process separates a sample from the person even within the confines of the single encounter standard (and even more so if the single encounter norm must be violated), then a process for certain identification of the individual and association of the sample with the individual is needed. Bar code technology and existing personal identifiers (*e.g.*, drivers'

license magnetic strips) can be of assistance in this task. The use of biometrics should also be explored.

With the exception of the person/sample identification technology, all of these technologies are judged to be high risk because no technology is readily available to meet the stated goals of emergency responders.

PHRBAE.3 – Modeling of Exposure and Containment. *The ability to predict the likely numbers and geographical distribution of individuals exposed to biological agents through modeling exposure to or containment of an agent.* The technology will help public health and safety officials manage emerging threat conditions by anticipating which regional areas and personal lifestyles are conducive to exposure to moderate to high levels of agent and thereby plan for prophylaxis, and quarantine, and for back-tracing contagion to its source(s).

The DIDA.6 (*CBRNE Effects Modeling and Simulation*) and MR.6 (*Modeling of Exposure/Casualties for Location and Numbers*) functional capabilities focus respectively on modeling atmospheric dispersion of CRBNE agents and effects and the illness resulting from exposure to chemical and radiological materials. The modeling of dissemination of biological agents after initial airborne dispersal, and their distribution through other channels, is addressed in this section. The major differences between biological agent dissemination and that of either chemical or radiological agents include the self-replicating nature of the biological agents and their very long survival in particular circumstances. As a result, persistent infection is a problem in certain exposed individuals. For highly contagious biological agents, infected individuals can serve as seeds for iterative dissemination of the agent and therefore cause multiple waves of illness. (The SARS epidemic has prompted research into the phenomenon of the "super spreader.") In highly mobile modern society, exposure of a small population in an airplane can lead to rapid distribution of pathogen globally. For zoonotic disease (transferred from animals to humans or spread by an insect vector) dissemination patterns are a function of the migration of the host and presence of the vector (such as West Nile Virus).

Goals:

Responders and public health officials recognize that they will be lucky to discover a biological agent release in progress. So the modeling software must have the capability to backtrack from emergent illness and epidemiological information to discern the initial dispersal mechanism and area. The system must also be able to model the likely pattern of infection from residual agent in the environment. It should predict likely demographic and geographic progression of an epidemic starting from information on the disease agent, its virulence, the current health status of the population, and other factors such as weather. In addition, it should also be capable of projecting the effects of such policy measures as quarantine.

The modeling capability to interpret information output during threat conditions must be available to responders and public health officials at the incident scene as well as command centers, and be accessed from mobile computers. The modeling information should have the capability to be integrated with other data sources and data users (including early detection/syndromic data, decision support for isolation/quarantine/containment, hazmat integration) and preferably be web-enabled. The operation of the modeling program should be graphical and easy to understand. The software should not require significant technical support on-site. The training of responders to use the modeling program should require four hours or less and the results of a modeling run should be available within one hour. The modeling system should utilize real-time meteorological data and be capable of managing multi-level security.

Current Capabilities:

The Army Medical Command has published a book that catalogues biological threat agents, prognosis of clinical disease from these agents and treatment protocols. The book is available in a

wireless form that can be accessed from a PDA. This material is prepared for physicians rather than public safety responders.

The airborne dispersal models discussed in DIDA.6 (*CBRNE Effects Modeling and Simulation*) generally do not consider the possibility of re-aerosolization of agent that has been deposited after an initial airborne dispersal, or that has been introduced into the environment through non-airborne means.

Crude epidemiological transmission models have been used to support exercises but are not typically deployed in incident command centers or in state public health headquarters.

State of the Art:

Communities around the U.S. monitor environmental air quality and study the dispersal of particulates in urban and rural communities. Included in this are the Houston Advanced Research Council (HARC) environmental air quality program and programs in the Los Angeles area. Similar data are collected in major European cities concerned about environmental quality. While the particulates monitored (*e.g.*, diesel emissions) have a significantly smaller size (0.1 micron diameter) than biological agents, the patterns of agent dispersal and distribution can be estimated by responders using appropriate technology. The Los Alamos National Laboratory (LANL) epidemiological program for toxic metals and threat-agent dispersal has modeled the diffusion of such materials in ground and surface water.

The CDC has modeled the spread of infectious disease in communities. Some of this is available through the Morbidity and Mortality Weekly Reports of CDC. Epidemiological models have been used in policy analyses of vaccination strategy.

Some of the cited data may not be readily available to the general responder community for reasons of security. The establishment of trusted individuals at major centers, who could access such data, may facilitate rapid transfer to personnel in the field as necessary. While extensive research has been performed by the defense community in agent dispersal there is a need to fuse military information with public health modeling and data sets.

Technology Limitations and Barriers:

The likelihood that a given dose of agent encountered by various routes will cause infection in humans is not well characterized. The relative susceptibility of young persons, the aged, patients with compromised immune systems (*e.g.*, AIDS, organ transplant recipients) remains to be determined. The number of anthrax particles believed necessary to cause disease in August 2001 had to be revised downward in 2002 because of an elderly woman in Connecticut who developed the disease. Almost all susceptibility data was acquired from models using healthy animals. The effects of urban crowding, nutrition, co-infection with other agents, and occupational status are confounding elements. Moreover, it is entirely possible that an incident will involve specially bred or engineered organisms that have virulence or toxicity different from the strains previously encountered.

The determination of which modeling system is to be used will affect training programs and the need to have consensus on national use of a specific model will delay implementation of this task. This is less a technology issue than a policy issue.

Gap Fillers:

The linking of early disease detection systems (*e.g.*, syndromic) with Global Information Systems and data/mapping is readily achievable. The electronic storage of archival disease emergence data, from state departments of health, can provide a basis for an analysis and review of lessons learned. The information of interest includes: the co-dependency of agents on other kinds of infection, the effects of demographic shifts on emergent disease and virulence changes in biological organisms.

Research is required to investigate the role of various societal and biological situations on agent dissemination and emergent epidemics. These

situations include how the living conditions (urban/rural), employment conditions (density, ventilation, humidity), transportation patterns and genomic markers affect the spread and virulence of the disease. The SARS epidemic in China revealed significant differences in susceptibility of various communities in affected areas to severe disease.

Many continuing research initiatives are relevant to this area and there are no particularly difficult technological questions in system development; the difficulties relate primarily to a lack of full knowledge on the modes of transmission and degree of virulence of the wide variety of threat agents that can be envisioned (some of them genetically engineered). Thus there is an inherent limit to the accuracy of the modeling that can be developed.

PHRBAE.4 – Isolation and Quarantine. *The ability of public health and safety officials to minimize the onward spread of infectious disease through the control of contact between unexposed and contagious individuals.* Isolation refers primarily to techniques for protecting healthy people from exposure to contagion even when they must be near and even interact with contagious individuals; quarantine refers to the enforced residential segregation of possibly contagious people.

The technology should support the identification of exposed populations and measures to ensure effective isolation of exposed and unexposed populations. This applies to potentially contagious populations both in and out of treatment facilities. This capability will permit establishment of care delivery facilities that will house thousands of patients in a secure, appropriate manner. MR.3 (*Individual and Collective Protection – health Care Facilities and Personnel*) discusses technologies and mechanisms to prevent the spread of contamination from threat agents within established medical care facilities (*e.g.*, clinics, hospitals). A significant portion of the population within these facilities is immunocompromised or otherwise more susceptible to disease (nosocomial infections).

Goals:

The emergence of SARS in China and Canada has heightened awareness of the need to develop a capability to isolate and quarantine individuals with serious contagious disease. There is an associated need to monitor the success of isolation. GPS monitoring of quarantined individuals would be an enabling technology for this goal, although it is also necessary to ensure that previously uninfected individuals do not stray into contact with quarantined people and places. Education of the public to achieve operational acceptance is also needed.

An important requirement is creation of an entity that can authorize orders for isolation and quarantine and can enforce such an order. At the present time the authority to quarantine resides in the state departments of health while enforcement resides with public safety organizations or the National Guard.

Current Capability:

In the period after recognition of a release of a biological threat agent in an urban area it will be necessary to process thousands of people. If hospitals and public spaces are to be used for isolation of patients with highly communicable disease, such facilities will need to be retrofitted with effective isolation capability (*e.g.*, positive and negative pressure and airflow). Very often the unintentional admission of a person with a highly contagious disease results in contamination of the hospital. For example, the air handling capability of many emergency rooms is directly connected to air handling in the whole facility. Containment then becomes a matter of security and exercise of authority—extremely contagious people must be kept out of the emergency room. A sensor which could scan people as they walk in and determine which persons were exposed would be very advantageous.[13] Screening stations may need to be established outside of the treatment facility itself. Patients with highly communicable diseases should be provided rooms with negative pressure to reduce dissemination of contaminated air throughout a

[13] Unfortunately, since very small numbers of certain kinds of bacteria or virus particles lodged within the body can bloom into a virulent and contagious infection, it is entirely possible that someone entering the hospital appearing to be "clean" could after a period of days in the hospital become a source of contagion without encountering any further agent within the hospital.

structure; other patients may be provided rooms with filtered airflow and positive pressure if there is high confidence that they are not contagious. Ideally each patient would be provided with filtered air and provision would be made for the removal of the bulk of the air from a room so that inadvertent spread does not occur. Related to this point is that most mobile or portable hospital units do not have the capability to regulate airflow in the manner needed to sustain negative pressure. Today, most hospitals do not have a significant number of isolation units.

New guidance on effective quarantine emerged from the SARS experience. The experience with SARS has been described in the CDC's Morbidity and Mortality Weekly Report (MMMWR) and provides good data on the Toronto experience showing how they did isolation and quarantine in schools and home- based and hospital isolation. Home care was provided for 350 individuals suspected of SARS. In addition, Canada prepared forms alerting deplaning passengers to the signs of SARS. The SARS response projects of Canada, Taiwan and South Asia are models for developing new approaches to biological threats in the developed world. Yet the rules of engagement for declaration of quarantine are ambiguous as was seen during the SARS event in Canada. Economic loss to the community and political requests to remove quarantine emerged. Standardized methods of quarantine enforcement remain to be developed.

State of the Art:

In the event of a severe outbreak of highly infectious disease the military uses field hospitals for mass quarantine rather than fixed facilities.

Architectural and engineering plans have been prepared to retrofit the emergency room facilities at the University of Pittsburgh for management of patients with highly infectious disease. The retrofitting includes placement of fans and HEPA filters. Other hospitals have been retrofitted or have plans to be retrofitted for such an incident. The CDC has prepared a report on lessons learned from the Toronto SARS event (schools, home-based, hospitals). The National Guard Bureau in 1999 prepared a report on the role of the NGB during quarantine and came to the conclusion that declaration of quarantine is problematic.

The most serious issues related to isolation and quarantine primarily have to do with policy and resources, not technology.

Technology Limitations and Barriers:

Policies and procedures for declaration of quarantine vary from state to state and are markedly affected by legal issues. There is a clear divergence between authority to declare a quarantine and enforcement of the declaration. Because of the expectation that a biological event will affect thousands of people, it appears clear that neither the U.S., nor any other nation in the developed world, has the capability to manage thousands of people ill with a highly contagious and lethal disease. The likelihood that the disease will emerge in a short time period (less than fifteen days) compounds the logistics of medical management. In addition to medical care there will be difficulties with enforcement of policy and maintaining security.

Gap Fillers:

Various federal entities have examined the role they may play in quarantine. The Department of Homeland Security is expected to participate in this effort and the National Guard has examined its potential role in the quarantine process. The success of the SARS efforts is likely to influence future quarantine processes.

Responders believe that current procedures for protecting health providers and responders are not adequate. However, a search for enabling technologies led to little more than air handling systems, locator devices, personal protective equipment for medical workers, and decision support tools—all of which are well within the state of the art. Needed sensor systems will be developed as part of other functional capabilities and NTROs.

PHRBAE.5 – Affordable Specimen Transport for CW and BW Agents. *Procedures and devices which provide the ability for transportation of potentially lethal chemical and biological agents and the availability and security of containers used to transport biological agent samples.*

Goals:

Emergency responders have a need to contain biological samples for shipment to a laboratory where they can be analyzed. The shipping containers (vials) must be affordable, cost less than $100, be available in multiple sizes and be able to sustain viability of living cells that are being sampled. The vials and shipping containers must be ruggedized (they should withstand a plane crash without dispersing agent). Training of responders is required for collection of the sample without disturbing a chain of evidence, packaging of the sample and addition of nutrients or other amendments to assure intact arrival at the analytical site. There is a particular need to address evidence and documenting the chain of custody.

Current Capabilities:

At the current time chemical agent samples are transported in salvage cylinders that cost about $6,000 each. Lawrence Livermore uses microfibers in a waterproof plastic case that is opened in a hot zone and then closed, decontaminated on the surface and transferred to an analytical laboratory.

The shipment of suspected or actual biological agents does not require such expensive packaging because no volatiles are involved. The biological samples are placed in sample vials, secured with an O Ring, placed in a zip lock bag and then packed using triple containers (each inserted into a larger container) and labeled as biohazard. The container can be manipulated despite limited dexterity of responders in HAZMAT suits. Some clinical specimens need oxygen, some refrigeration, and some positive pressure. The size of the sample is frequently small but may vary and include large sample volumes. The cost of shipping and containers is less than $100. Federal Express now knowingly transports these hazardous samples.

The responders indicated that the average fire department does not have the money to purchase the available biohazard containers. If federal funds are not provided, the realities of today's fiscal climate mean that local governments will not purchase the vials even at low cost. Responder departments that have special operations capabilities typically have one or two containers. There was a perceived need for readily available procedures, protocols, and shipping vials for sample recovery

State of the Art:

Several federal agencies and commercial organizations have standardized protocols for the shipment of biological samples (*i.e.*, USAMRIID, CDC, American Type Culture Collection [ATCC]). The U.S. Department of Transportation (DOT) describes protocols for sample shipment and carriers that can safely transport such materials.

Technology Limitations and Barriers:

The shipment of biological agents does not require new technology development. The majority of samples to be analyzed for the presence of biological agents are small in volume (under 50 milliliters).

Although responders do not have appropriate containers, such containers are available and routinely used. While no RTO is associated with this functional capability, the Department of Homeland Security should review the market availability of affordable appropriate containers and establish standards and guidelines for responder stocking of these containers.

PHRBAE.6 – Transport of Contagious Patients. *The ability to transport multiple contagious patients without endangering medical care providers or the public.*

Goals:

Responders want access to single-patient mobile isolation environments that are cost effective (priced below $1500), have disposable liners, are easily deployed and non-stressful to the patient. The unit must allow clinical assessment and critical interventions by multiple providers, be user friendly and require less than one hour of training of emergency responders for appropriate use. It should be light-weight and easily processed for decontamination, and be accommodated on a standard ambulance stretcher.

It should accept a full range of patient sizes (pediatric through obese) and those with special needs. It should be self-sufficient with respect to power for at least two hours and allow for administration of life support oxygen. In the best of circumstances the unit should be able to accept a new patient after fifteen minutes of decontamination. Such a device should be introduced into the National Pharmaceutical Stockpile.

Current Capability:

Patient isolation systems for use in transport are not currently in use by emergency responders, and are not deployed in quantity by the Department of Defense or other federal agencies.

There are no standards or accepted protocols for transporting hundreds of patients infected with a highly contagious lethal disease. Affordability is a big barrier for acquisition of the pod systems. Because current policy strongly recommends against the movement of patients who are infected with a highly contagious biological agent, reconsideration of this guideline in conjunction with analysis of technological options would be needed before transportation isolation systems would become a critical item for biological defense in the United States.

State of the Art:

The Department of Defense has invested in the development of systems that facilitate transport of very ill (especially trauma) patients and other systems that permit transport of persons infected with highly contagious agents. These systems are designed for long-range air transport, which imposes requirements that may not be needed for metropolitan emergency response.

USAMRIID has a small number of Aeromedical Isolation Teams to safely transport patients with lethal communicable diseases from the field into USAMRIID containment facilities. The teams are equipped with flexible clear plastic enclosures on wire frames with battery-operated negative-pressure air filtration systems and glove boxes. These come in two sizes—a stretcher size unit that can be carried by two people and a larger air transportation unit that facilitates in-flight medical care.

The Life Support for Trauma and Transport (LSTAT) is an individualized portable intensive care system and surgical platform providing resuscitation and stabilization capability through an integrated suite of state-of-the-art medical devices. It is designed to decrease mortality, morbidity and disability by moving trauma care farther forward toward the site of an injury for improved diagnostics and therapeutics throughout the evacuation and treatment process. The current, third generation, LSTAT, features a ventilator, suction, oxygen system, infusion pump, physiological monitor, clinical blood analyzer, and defibrillator. These medical devices are complemented with a fully network-capable on-board computer monitoring system and stand alone power system all packaged together in the NATO litter form factor. However, owing to the small numbers of systems (around 25) currently field-deployed, the systems tend to be used more as mobile forward patient support systems in austere environments rather than end-to-end transporters. The price of the system ($165,000) is also an obstacle to widespread use. The high-end medical support features would often not be required for transport of patients who are contagious but stable. Although the current LSTAT does not have isolation capability; the next-generation LSTAT, currently in development, will be available with a canopy and negative and positive pressure and filtering for isolation of contagious and “clean” patients (respectively).

The Alion Corp has a product that involves placing the patient in a contained elastomeric unit with capability to administer critical gasses including oxygen.

Technology Limitations and Barriers:

Design of such pod systems is fairly straightforward. Tradeoffs between cost and levels of capability must be addressed in the context of preferred concepts of operations for where and how patients would be treated. It would be worthwhile for the Department of Homeland Security to host a demonstration and standards development process that would help coordinate a market for vendors of such systems.

PHRBAE.7 – Safe Handling of Medical Waste.

The safe handling and disposal of large quantities of unusually infectious medical waste, for use in homes and alternative treatment facilities as well as doctors' offices and other established medical care facilities. In a situation following massive outbreak of disease with a highly contagious and lethal biological agent, the large volume of contaminated materials would pose a major logistical problem. The rate of accumulation of contaminated materials and large volume differentiates scenarios involving biological agents from what we do today. Medical waste includes used needles, blood and pus, absorbent materials from diapers and sponges, bandages and dressings, and human excretory products. Among the components that could mitigate the management problem are special vehicles or containers configured to fit existing vehicles. High tensile strength disposable materials must be used because infected individuals may be self-administering drugs with needles and current practices may result in improperly covered sharp pointed objects which can poke holes in trash bags. The disposal bags and processing must be affordable, but may be third party reimbursable.

Responders recommend including waste-handling supplies in the stockpiled push packs.

Goals:

The potential magnitude of the waste suggests the development of interoperable containers for hazardous trash that can be used by existing infrastructure in major medical centers and hospitals. The containers require minimal handling, must be rugged and able to contain most dangerous organisms. Safe storage would be required until disposal capacity can be arranged.

Training of home health care providers for use of these containers should require less than ten minutes. The containers must be part of a national stockpile and part of all home care kits. This is a logistics issue, with education and procedural components.

State of the Art:

Existing products for home health care currently exist.

Technology Limitations and Barriers:

There are no technology or cultural limitations or barriers. No RTO is defined for this functional capability.

Public Health Readiness for Biological Agent Events Response Technology Objectives (PHRBAErto)

PHRBAErto.1 – Health Surveillance for Early Detection of Biological Agent Events

Objectives:

Develop a comprehensive surveillance system that ensures initial recognition of an emergent illness at the earliest point in the progress of a biological agent event. This system would be based in metropolitan and regional areas but would allow fully transparent data aggregation up to the national level. Near-real-time data sources would include work and school absences, over-the-counter and prescription pharmaceutical purchases, syndromic information on clinic, doctor, emergency room and hospital visits, 9-1-1 and EMS calls, and information from veterinary sources and medical examiners. It would encompass historical data sets and regional demographics, commuting and travel patterns to support full data mining capabilities, and forward links into epidemic modeling capability. It would have a full set of iconographic, geographic, and temporal display modes

and semi-automated and automated modes for correlation of data bearing on emerging clusters of illness and their statistical significance compared to base rates. The system would also provide alerting functions for further epidemiological investigation and for policy interventions.

Payoffs:

There is a 48 to 72 hour lag between initial exposure to an agent and appearance of clinical signs. Medical interventions with antibiotics/antivirals, vaccines or containment of the exposed persons during this window can greatly diminish the number and severity of subsequent cases of illness. Early recognition will lead to early identification of the pathogen; once an infectious illness is identified, further occurrences can be more readily identified and treated.

The result will be a decrease in the number of patients that will acquire the disease from secondary or tertiary exposure and a decrease in the severity of illness in those persons exposed to the agent initially. Of course, a powerful health surveillance of this sort would help in dealing with natural as well as deliberate public health threats.

Challenges:

A key challenge is identifying emergent disease in a cohort sufficient in size to reduce false positive/negative data sets. A large number of patients are needed and this can be achieved by networking multiple hospitals/clinics in a regional system. However, the ability to detect small initial clusters (ideally) of pre-clinical illness against this background requires sophisticated data mining tools. In addition to alerting, the system must allow rapid revealing of patient identifying information for further investigation, while maintaining patient privacy under normal circumstances.

The surveillance data must be acquired in near-real-time without additional effort by the health care providers. This is a medical economics issue. A surveillance system based on capture of electronic medical data, from which all individual identifiers have been removed, can be devised to protect patient privacy. However, sufficient identifying information must be held in reserve for rapid exploitation in fast follow-up epidemiological investigation once disease clusters have been recognized.

Cost/benefit research will be needed to determine the types of data sources to be included in the deployed system and the level of detail that should be reported. Careful attention to architecture will be required so that useable systems can be brought up quickly with provision for them to evolve gracefully into a fully powered integrated system over time. Different regions will have different starting points and needs and so the system will definitely have to tolerate diversity.

Milestones/Metrics:

FY2004: Benchmark epidemiological early warning research to date. Survey public health databases and select data sets appropriate for these purposes. Harmonize diagnoses and other information codes used in these systems. Using the best practices of existing research efforts, begin design of an Syndromic Surveillance and Response Prototype. Initiate research on new methods of automated population of health care databases (*e.g.*, automated diagnostic labs with real-time links to syndromic databases – see PHRBAErto.2 (*Rapid, High Throughput Clinical Assessment and Testing*) and the Strategic Research Area on *Biomarkers of Agent Induced Disease and Systemic Injury*), for possible eventual inclusion in later versions of the system.

FY2005: Deploy Syndromic Surveillance and Response Prototype initial capability (perhaps at three sites with different demographic characteristics); establish minimum standards for interoperability, data formats, and provisions for display and analysis. Begin test and evaluation of prototype in three cities. Continue research into value of disparate data sources and integrate into prototype as appropriate. Continue research into automated syndromic data generation.

FY2006: Conclude research on value of disparate data sources. Continue testing and evaluating prototype system. Develop improvements to the

prototype based on test results and data access and generation research.

FY2007: Finalize interoperability standards for Syndromic Surveillance and Response systems. Increase deployment and testing of prototype to several more metropolitan areas. Continue research into automated data gathering and integrating results of that research.

FY2008: Finalize Syndromic Surveillance and Response System architecture, design and tools. Demonstrate target capability nationwide. Assess results of research on automated diagnosis and reporting for inclusion in future version as appropriate.

PHRBAErto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Early Detection	$20	$30	$45	$60	$50	**$205**

PHRBAErto.2 – Rapid High-Throughput Clinical Assessment and Testing

Objectives:

Improve the speed, throughput, comprehensiveness, and convenience of clinical assessment and testing for characterization of biological agent exposure and disease status, in the three contexts identified in PHRBAE.2. Draw on the Strategic Research Area, *Biomarkers of Bio-Agent Induced Disease* (see Chapter I), to develop additional, non-invasive, approaches to screening and diagnosis.

Payoffs:

Such an improved capability would significantly improve the likelihood of early recognition and accurate characterization of a biological-agent induced epidemic, with substantial benefits in reduction of morbidity and mortality. Depending on the context, it may also: improve the accuracy of treatment, improving results and reducing the threat of side effects; improve the efficiency of efforts at isolation and quarantine, further reducing the scope of an epidemic; and reduce exposure of health care workers and responders to threat agent and permit responders to operate with reduced protective gear. By improving the speed and accuracy of ordinary medical diagnosis, faster clinical testing will also improve the power of the health surveillance system, even apart from its direct role in diagnosing biological agent induced illness among patients in doctors' offices, emergency rooms, and clinics. Finally, the technology for rapid diagnosis would improve health outcomes and reduce medical costs in the absence of a biological agent event.

Challenges:

No combination of current technology exists to provide the combination of speed and stand-off desired by responders. Fortunately, achieving much of the payoff identified does not require reaching this level of capability.

However, no other context is likely to place the emphasis on minimal contact and on speed as the role of screening for exposure to biological agents; so this should have a special priority. At the same time, there would be such a high payoff for accurate clinical blood tests that would take even an hour or more that this avenue is also important to explore.

As compared to naturally-occurring disease, biological agents may be engineered to circumvent detection; this possibility needs to be taken into account and may bias the preferred approach in favor of genomic tests instead of immunoassays, even though these tests tend to take more time.

Finally, there is likely to be an interval after exposure where no minimally invasive test will identify 100% of those who may become ill. Also, attempting to identify agents before they rise to the level of major infection means that the test will face a very high background noise level of other microorganisms. Many biological agents will be hard to distinguish from similar non-pathogenic organisms. For all these reasons, achieving the ultimate level of capability cannot be the sole focus of this RTO.

Because of the strong overlap with normal medical practice, agencies of HHS, including the National Institute of Allergy and Infectious Disease, and the CDC, should be directly

involved in the development of programs under this RTO, together with agencies with expertise in threat agents.

Milestones/Metrics:

FY2006: Review progress of Strategic Research (see Chapter I) into the outward physiological signs of exposure, disease and injury. Review current research and technology developments in minimally invasive rapid testing techniques. Begin developing an architecture and strategy for designing a Rapid High-Throughput Clinical Assessment and Testing System (RHTCAT), at first with minimally invasive techniques and later with non-invasive techniques.

FY2007: Issue a Broad Area Announcement seeking several approaches to designing and building RHTCAT.

FY2008-2010: Award several contracts to develop promising approaches. Test and evaluate several competing prototypes. Begin commercialization and clinical testing efforts on the most promising approaches, most likely through partnerships with established medical diagnostic suppliers.

PHRBAErto.2 – Budget in Millions

Thrust	2006	2007	2008	Totals
RHTCAT	$15	$30	$40	**$85**

PHRBAErto.3 – Models for Re-dissemination and Contagion of Biological Agents

Objectives:

Develop improved models for the re-dissemination and contagion of biological agents. The major differences between biological agent dissemination and that of either chemical or radiological agents include the self-replicating nature of the biological agents and their very long survival in particular circumstances. The models must be integrated with surveillance information (PHRBAErto.1 (*Health Surveillance for Early Detection of Biological Agent Events*)) to help get a starting point. They must also encompass policy options such as quarantine and treatment to see the effect on projections.

Payoffs:

All biological agents, with the exception of toxins, will replicate in a host. As a result, persistent infection is a problem in certain exposed individuals. For highly contagious biological agents, infected individuals can serve as seeds for iterative dissemination of an agent and therefore cause multiple waves of illness. The payoff for success in this task may be the reduction in severity of illness in potentially infected persons and the elimination of subsequent waves of illness in individuals coming in contact with the initial target population.

Challenges:

Modeling of this sort faces three primary challenges. First, accurate predictions would require very detailed data about initial exposure and future patterns of interaction, which would be difficult to get. Second, because the models attempt to capture events of a sort that have never happened, the estimated parameters of contagion and survival are likely to be wildly inaccurate. Finally, for many of the biological agents, we do not have human infectivity or lethality doses. Extrapolation from old data or inappropriate animal models is insufficient. (Moreover, a biological agent event may involve a wholly new variant of an existing organism.) In the interim, the modeling and simulation community must continue to refine the physical, chemical, meteorological effects and other parameters that do not rely on human effects.

Therefore, the main challenge will be to keep the modeling at a level where it is relevant to policy and not to expect it to be an exact, "validated" reflection of reality.

Milestones/Metrics:

FY2004: Survey existing models and define appropriate performance levels. Identify gaps in capability needed to accomplish goals. Develop strategy to fill the gaps.

FY2005: Issue a Broad Area Announcement seeking an advanced technology demonstration

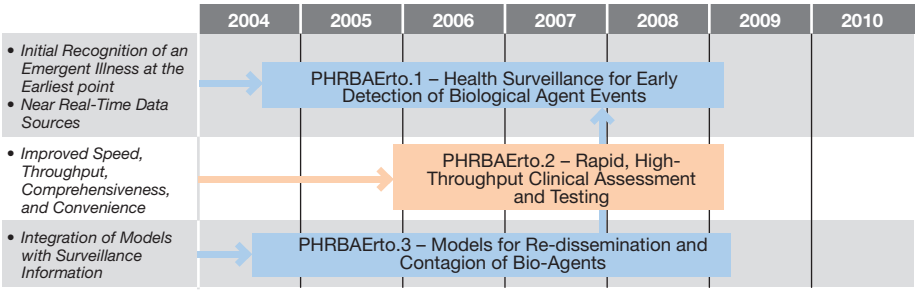
using the strategy developed. Evaluate BAA responses and choose one or more performers.

FY2006-2007: Develop Bio Contagion Modeling Tool. Conduct field demonstrations and finalize specification for deployable system(s).

FY2008: Begin to transition final capability to users.

PHRBAErto.3 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Bio Contagion Modeling Tool	$10	$25	$40	$40	$40	**$155**



Public Health Readiness for Biological Agent Events (PHRBAE) Technology Roadmap

Chapter IX

Logistics Support (LS)

Chapter Chair: Dr. Lou Mason
Chapter Coordinator: Dr. Maria Powell

Definition

Logistics Support is the capability to deliver equipment, consumables, food, water, other supplies, shelter and transportation when and where needed in support of emergency response to a terrorist incident.

Several aspects of this definition should be kept in mind. First, many functions that would be viewed as logistics in a military operation overseas do not appear here because they are primarily civil support rather than support to the response *per se*. Functions of ordinary civil society such as traffic management and water and electricity are covered in other NTROs (Emergency Management, Response and Recovery, and Medical Response) and not in logistics. Second, this NTRO primarily addresses the ability to deliver support to responders rather than the support itself. It is the marshalling of the supplies rather than the supplies themselves. Finally, the NTRO focuses on aspects of logistics that can be enabled by technology; much prosaic supply and maintenance activity does not get specific mention as a result. For example, the NTRO does not address the pre-positioning of supplies or the pre-loading of purpose-specific pallets of supplies.

The specter of catastrophic terrorism requires that disparate responder organizations – ones that normally do not work closely together – must learn to operate together. Efficient interoperation requires consistent procedures and equipment standards. However, inconsistent policies, specialized responder needs, limited budgets, imperfect communications, and restricted training all limit the success of current logistics operating procedures. While technology is important to achieving the ultimate level of desired performance, standardization of procedures and items would improve performance even without an infusion of new technology. The process of deploying an affordable technology-based tool can work to harmonize procedures as well as providing more rapid, more precise, and more comprehensive logistics management, and thus better support to emergency responders.

Operational Environments

Logistics is the process of supplying, transporting, maintaining, and servicing all elements of the responder's capabilities. In evaluating logistics functions, responders thought it more useful to distinguish between phases of the response rather than the type of attack. They thought that there was likely to be as much variation in logistics requirements within a particular attack category as between categories. Responders focused on needs to ensure a high state of readiness prior to operations through the use of deliberate planning, to provide support during the initial response to an incident, to provide tailored support as the specific requirements of an incident emerge, and to rapidly reconstitute logistics capabilities at the conclusion of the incident. These phases are conveniently labeled: pre-crisis deliberate planning, post-event initial logistics response, adaptive execution, and logistics recovery.

Throughout these phases of an incident, there is the need to effectively anticipate requirements, communicate among jurisdictions and organizations, manage transportation and other logistics processes, and optimize assets. Due to the variety of responder disciplines and organizations, policies, procedures, and equipment in a given location are not standardized and often not interoperable. The lack of standardization of equipment

complicates the provision of consumables such as batteries and service items, which may vary according to the type of equipment. This difficult situation is likely to be further complicated by a lack of trained logistics personnel and effective logistics command and control procedures. A language barrier often causes additional difficulties and delays: naming conventions often create confusion, especially when communicating a critical need where specificity is paramount. Responders cited the need to not only coordinate logistics operations internally, but also with external organizations (other responders, federal, state, and commercial) throughout the planning, execution, and reconstitution processes.

Needed Functional Capabilities and Priorities

Listed below, in declining priority order, are the logistics functional capabilities required:

- Logistics Information System
- Automatic Generation and Assessment of Supply Requirements
- Inventory Management
- Mortuary Affairs Management
- Lightweight, Long-lived Power Sources
- Transportation Optimization
- Assessment of Safe Air, Sea and Ground Bases of Operations (Supply Depots)

Responders rated the *Logistics Information System* (LS.1) capability well above the rest in priority; the *Automatic Generation and Assessment of Supply Requirements* (LS.2) was solidly in the second position. Only the last capability received a majority vote as a low priority; the other four capabilities received mixed values.

In examining how these capabilities can best be improved, technologists and responders participating in the technology workshop determined that, to the extent that capabilities identified in the FCEs are susceptible to improvement by technology, the gains will be realized most expeditiously if these capabilities are addressed essentially as modules of an *Integrated Logistics Information System.*

Overall State of Technology for Logistics Support

The matrix below summarizes the readiness of technology to underpin capabilities for Logistics Support.

The predominance of green in the inner boxes means technologies needed to support functional capabilities in most of the operational environments are within reach; the preponderance of yellows and greens in the intermediate boxes means that there are few gaps that are believed to exist

Logisitcs Support

Functional Capabilities	Operational Environments: Pre-Crisis Deliberate Planning	Post-Event Initial Logistics Response	Adaptive Execution	Logisitics Recovery
1. Logistics Info Systems				
2. Automatic Generation and Assessment of Supply Requirements				
3. Inventory Management				
4. Mortuary Affairs Management				
5. Lightweight, Long-lived Power Sources				
6. Transportation Optimization				
7. Assessment of Safe Air, Sea, and Ground Bases of Operations (Supply Depots)				

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

between the capabilities that are needed and the expected results of commercial and government development programs already in train. This is because of the close relevance of both commercial and military logistics systems in meeting responder needs. Even for the *Logistics Information System* (LS.1), the red coloration of the innermost boxes was governed only by a few "ideal" capabilities; dramatic capability improvements compared to today were judged to fall well within the gambit of existing technologies.

LS.1 – Logistics Information System. *The capability to provide response commanders at various levels accurate and timely information on supply availability, resupply needs, and logistics resources and to allow them to manage the flow for optimum response effectiveness.* Access to the LIS by commanders and other elements of the logistics system must be standardized, interoperable, and affordable, and the LIS must be capable of:

- Accurate and timely logistics data capture and information fusion.
- Real time mission response asset accountability and tracking for personnel and equipment.
- Current supply usage and demand tracking and communication.
- Distributed visibility into the pipeline.
- Assured real-time logistics operational management.

The need for such an integrated logistic information system is paramount, to ensure that responders on the incident scene are maximally effective and that the effort to supply everything they might need (in the absence of good information on the actual needs) does not become an obstacle to other elements of the response.

Responders need an affordable solution, with the inherent flexibility to track assets (people, things, supplies) in real-time with a high degree of accuracy for their location and status. (Many of the inputs would be provided by sensors and communication channels developed under other NTROS—for example the responder location and health status monitors discussed under UIC, the various attack characterization technologies discussed in DIDA and the smart breathing apparatus and protective clothing addressed in PPE.) The LIS should provide a collaborative planning and management environment, allowing appropriate responders and officials at various levels to address logistics issues via voice and data, sharing a common logistics picture of the current and projected status of assets and flows.

In other words, responders want a flexible, adaptive, and easy means to share a blueprint of the situation (like a scalable map of an area – the picture), the ability to mark (draw and annotate), and the ability to aggregate and drill down on content (data and information). All responders and technologists realize that this need cannot be met by imposing a standardized, one-size-fits-all system across the variety of responder domains, cities, states, etc. By paying attention to an open architecture and interoperable systems, many of the information system needs can be met by decision support tools that require minimal training, permit reliable access to information, and provide synchronous and asynchronous collaboration.

In the pre-crisis phase, the LIS would function to facilitate deliberate planning and simulated and physical exercises of logistics response across jurisdictional and disciplinary boundaries. In the immediate post-event phase, the LIS would help commanders tailor and manage the initial logistics flow, mostly based on pre-planned options. The LIS would enable an early transition to the adaptive execution phase, in which the logistics response is closely matched to the actual needs of the event rather than to pre-planned scenarios.

In the adaptive execution phase, the LIS would incorporate up-to-the minute inputs both about the evolving nature and scale of the event and the needs of responders on the scene to recalculate logistics needs. Finally, the real-time tracking provided by the LIS will support an earlier, more accurate, and less-costly repositioning of logistics assets and reordering of consumables, resulting in an earlier and more efficient recovery of full logistics capability.

Goals:

The LIS must meet responder needs in three areas: performance, integration with broader incident management systems, and openness to all response organizations. The performance goals relate to the ability of the system to collect, track, and present information relevant to projecting detailed logistics demand, tracking and displaying logistics flows and assets, and planning and managing the deployment of logistics assets to meet the demand over the full course of the response. The LIS must function as a part of a broader incident command system and supporting software, for the most part running on the same hardware and using the same communication channels and protocols. Finally, the LIS must be flexible and open (while remaining robust and secure) so that it can accept demand, flow, and asset information from and allow planning participation by all response organizations, including all responder specialties, all regional responder departments, volunteer personnel and private-sector assets, as well as FEMA and other federal government participants.

Ideally, all response and regional and federal government organizations would be included, integration with the incident command system would be seamless, and the status of all personnel and equipment (no matter what jurisdiction or organization they belong to) would be tracked automatically along with their projected demand for consumables. Similarly, all supplies and transportation and storage assets would automatically communicate their availability, location, and other relevant attributes to the LIS on a real-time basis.

In practice, of course, significant improvements over current capabilities could be achieved by systems that fall well short of meeting these ideal goals. Because of the mix of systems that different jurisdictions, agencies, and vendors will have in place, the LIS must provide interfaces for tracking and marshalling assets that are not equipped with the most modern reporting capabilities.

Current Capabilities:

Today, the logistics function is not generally recognized as a separate discipline. Automated tracking capabilities are non-existent in most responder contexts. Although some jurisdictions have established bar-code tracking for materials over a certain value ($500), these are not typically integrated across disciplines and jurisdictions. Responder personnel are typically tracked by blackboard or at an aggregated (squad) level. ICS (incident command system) software exists but is unaffordable for most jurisdictions and not standardized.

Information integration and scalability are current limitations to the effectiveness of logistics management across responder domains. Capturing and managing data and knowledge is difficult and limited. Information on the status of equipment readiness and inventories is virtually non-existent, and where information exists, the lack of accessibility, transparency and interoperability makes the information of little value to external elements.

State of the Art:

The current state of logistics information systems is evolving at a rapid rate, both within the commercial supply chain and also in government. In addition to full visibility of assets and goods in transit, the trend is toward increased integration, collaboration, and adaptability. Making information systems completely Web-accessible reduces the significance of boundaries among organizations and functional domains. Data integration, mining, and mediation technologies are permitting the use of data residing in legacy systems, even with differing semantics and schemas, to be accessed and combined in near real-time without special-purpose programming. High resolution graphics and visualization capabilities permit users to create customized views of information for collaborative analysis via the Web.

Tagging and sensing mechanisms (bar codes, radio-frequency ID tags, etc.) are becoming cheaper and more reliable, as are mechanisms

that automatically report on the status of mechanical systems and power sources. Finally, discretionary access control and role-based customization is evolving as a standardized feature in decision support tools to permit a level of security and prevention of information being misused or interpreted out of context. The major challenge in the responder domain is to obtain a capability that can be put at the disposal of a critical mass of users to ensure stability, providing strong incentives for cultural issues to be resolved.

Today, responder logistics command and control does not take advantage even of yesterday's technologies, not to speak of tomorrow's. Emerging technologies will permit greater flexibility at a lower cost. The key to leveraging state-of-the-art software is integration and user access, permitting users to tailor products to meet multiple logistic functions with the level of specificity required to forecast needs, make decisions, prioritize assets, and monitor readiness during any phase of an incident.

The military has invested years in evolving and customizing logistics capabilities. Current trends see the military looking to the commercial supply chain for inventory, transportation, optimization, management systems, and business practices. Commercial supply chain practices, born in the "lean" or "just-in-time" manufacturing ethos and the Wal-Mart lean inventory, low-margin, customer focus, facilitate reduced inventory and delivering the right product at the right time to meet customer demands. Tracking of shipments is critical and anticipation of needs is being accomplished with an unprecedented level of accuracy. Small businesses who have limited resources have turned to third party logistics providers (3PL) to provide support (parts and transportation) for low density critical resources. 3PL providers have moved into a global broker position to make the best of the competitive markets.

The military has realized the value of this concept with the creation of the Defense Logistics Agency's EMALL (electronic commerce mall) permitting consumables to be identified, located and purchased via the Web. This medium has reduced government inventories, reduced ordering and financial paperwork, increased customer satisfaction, and optimized transportation time. It has also permitted greater vendor participation and competition. An EMALL for responders could identify, locate, and purchase items to meet incident needs, in the quantities required, without having to hold significant and costly inventories locally, let alone be burdened with additional decisions in times of crisis.

Commercial supply chain management solutions exist that could be readily adapted for use by responders to meet many basic and collaborative needs. Short of the single EMALL concept, regional or national organizations could standardize the interfaces between responder organizations and vendors and other logistics asset providers, to provide visibility into supplier pipelines. One way of doing this would be to provide incentives for vendors to use customized plug-ins for customer relations management (CRM) software packages. Optimization tools for transportation routing and movement planning could provide responders the ability to integrate a myriad of organizations supporting an incident into a common picture to set priorities and maximize utilization. Companies like i2 and Manugistics are leaders in this arena supporting large organizations like FEDEX, UPS, Dell, etc., in meeting transportation optimization needs.

Technology Limitations and Barriers:

Communications connectivity must be assured for the LIS to be effective. Managers of logistics response during an incident will have to compete for limited communications resources. While logisticians might prefer the autonomy of dedicated communications, it is easier to provide redundancy, security, and communications assurance as part of a unified communications system. Since responder logistics and overall incident command must interact frequently and be synchronized, it makes sense for the communications to be effectively seamless.

Responders are not satisfied with the level of experience and training that characterize the

people who end up fulfilling logistics tasks in a crisis. Modern systems have more complex logistics demands, requiring more sophisticated systems and managers. Training across boundaries, both practical and cultural, is required with any implemented systems solution. While training and integrated exercises are costly, this cost is mitigated if the systems developed for terrorist incidents are put in use every day. Responders and technologists agree that any information system should be used on a day-to-day basis and must serve equally well throughout the operational environments of the planning and execution continuum.

Any system must be scalable and able to retrieve and mediate data from disparate sources without the need to cache at fixed points. Also, data may require integration and downloading to local clients for immediate use while not connected to networks.

Integrating tracking technologies is difficult and demands continued testing for interoperability, reliability, and scalability. Responders worry that today's technologies for tracking are not mature enough to eliminate risk to life and mission. However, the limited logistics throughput in a crisis means that even with some risk of breakdown, an improvement in visibility would increase the reliability of the right supplies arriving. These risks are arguments for good practices, for testing and for backup operational methods, not for avoiding the use of modern techniques for tracking critical assets during execution.

Gap Fillers:

In the short term, several initiatives could enhance logistics information systems available to Responders:

- Establish a Web presence to disseminate experience with logistics in exercises and incidents, and to engender discussion of best practices and appropriate lessons. An initial national capability could be provided within a year for under $2M. This could be tied to MIPT's Best Practices – Lessons Learned Knowledgebase effort.
- Establish standard interfaces for COTS tracking capabilities (bar codes, RFID) ($5M over two years).
- Evaluate commercial and military candidates for inclusion in a semi-automatic suite of logistics decision-support and command and control system ($5M over two years.)
- Establish a robust server infrastructure on the Internet as the medium for collaborative logistics information systems. A mesh of cooperative servers could be established at a cost of $1M a year over 1-2 years. This should be done in conjunction with filling other secure responder collaboration and communication needs, as described in Chapter IV (UIC).
- Integrate commercial products and the above gap fillers – approximately 2 years at a cost of $6-10M.

In addition, the following longer-term initiatives could be started:

- Evaluate the benefits of an *automated* logistics command and control suite of decision support products, with software agent technologies for search and optimization. Such a system could be developed and fielded within 5 years at a cost of $40-120M, depending on the level of fielding and training. The big problem here is the need for automated domain bridging by software agents. Such a project should involve agencies such as DARPA to ensure that emerging information and communication technologies would be considered where appropriate.
- Evaluate the possible benefits of a next-generation, higher-resolution, longer-distance tracking capability, not hindered by interference (using ultra-wideband, mesh net, orthogonal frequency division multiplex (OFDM), and related technologies). Fully evaluating such a capability would be possible within 3 years at a cost of $5-10M; it could perhaps be deployable in 10 years at $50M. This is a high-risk S&T endeavor with global implications.

The next-generation tracking capability, and to a lesser extent the automated domain-bridging aspects of the command and control decision-support suite, are high-risk; without these elements the overall level of technical risk for LS.1 would be moderate and the increase in logistics performance from the intermediate technologies (COTS tracking and expert-guided decision support systems) would still be dramatic compared to current practice.

In addition to the high technical risk, there is the question of what could be called commercialization risk. This is the equivalent of Sony's technically superior Betamax videocassette format – a technical success that even its inventors do not use because of the dominance of VHS in the marketplace. Because of economies of scale as well as the need for interoperability, responders could not afford to buy a logistics system based on components that differ from those in use in commercial and military systems; thus the success of the next-generation tags would require that they would be adopted into military and commercial systems before being made available to responders. But it seems unlikely that the responder tail could wag the commercial and military dog in this way unless their requirements were very similar; if the requirements are so similar then it is unclear why the larger commercial and military R&D budgets would not result in off-the-shelf products that could then be adopted by responders without any substantial DHS R&D investment. Thus all that may be required in these advanced areas is a mechanism for inserting a responder voice into the counsels of military and commercial decision-making.

LS.2 – Automatic Generation and Assessment of Supply Requirements. *The capability to help responders forecast needs, identify sources, prioritize requirements, and order supplies.* Additionally, requirements for sustaining an incident must take into account the type of incident, weather, duration, available transportation throughput, and order/ship times. Responders need a decision support tool for meeting this need that is intuitive, helps determine requirements, maintains accountability, and can automatically generate requests. Responders agree that no incident is like another, but that a capability must be available to generate requirements that have a high degree of accuracy for meeting projected needs; in other words the system must "learn" from previous endeavors and make reasonable recommendations of supplies required in scope and time.

Goals:

- Develop an acceptable nationally recommended and standardized database/system to generate requirements appropriate for specific CBRNE. The information needs to be user-friendly, consolidated and formatted to fit specific incidents, command organizations, and logistics systems and suppliers.
- Provide capability in execution phase to re-supply in real-time with just the right supplies so as not to overburden a staging system. Coordinate private donations and on-scene procurement (Wal-Mart, Home Depot, etc.).
- Interface with Logistics Information System and its tracking element as well as the Incident Commanders' operational plans.

Current Capabilities:

This capability, as defined, is largely unavailable to responders today:

- Very limited baseline requirements information exists for explosives, incendiary and chemical incidents. Information exists to a lesser extent to meet biological and radiological incidents.
- In all cases, information retrieval is problematic.
- During execution, assessing requirements is manual and reactive – tools are non-existent to provide options, let alone determine, source, and order sustainment.
- No capability exists nationally for responders from varied domains to access.
- Some capability exists within FEMA and the USAR to pick sustainment items and find

sources of supply; however, the programs do not generate projected sustainment based on specifics of the subject incident.

State of the Art:

Both the Army and USMC have built requirements-generation products for meeting wartime scenarios. The Joint Theater Logistics ACTD (DARPA) has created collaborative Web-based aides that do requirements generation for mission needs based on force structure. Commercial supply-chain systems tend to be oriented to repetitive operations rather than one-of-a-kind incidents; thus there is no single off-the-shelf system that performs this task.

Technology Limitations and Barriers:

Creating a flexible decision support tool for requirements generation is not limited by technology. The ability to field, integrate, and ensure interoperability of such a capability are the only challenges. Additionally, this capability must be orchestrated to work in concert with a logistics command and control and information system.

Gap Fillers:

Using COTS products, software could rapidly be adapted to this need and fielded. This capability would have to link to commercial sources for placing orders and managing shipments. Software could be accessible for download via the Web and use Web-based interfaces for generating requirements, sourcing, and monitoring of orders. Additionally, the software must continually update historical "knowledge" for types of incidents, commodities used, and shortfalls. This capability could be provided to responders within 2 years for approximately $15M. The right approach is to build this capability in as a module in the LIS.

LS.3 – Inventory Management. *The ability to manage sustainment inventories, ensuring stocks are rotated, consumed prior to shelf-life expiration, and optimized for best use.* In addition, responders desire to maintain minimal stocks, while not failing to meet emergency needs, at the least possible cost.

Goals:

- Develop a category-based, interoperable, inventory management system that can be made mission-specific, affordable, and accessible.
- System must be easy to use, shared across jurisdictions, and data continually updated and accessible.
- System should interface with the LIS.

Current Capabilities:

Inventory management systems that span organizational boundaries are not used by responders today. Current practice has the following characteristics:

- *Manual* – use of whiteboards, markers, etc.
- Local commercial sources required to fill emergency orders, if stocks are available.
- Some jurisdictions have limited inventory management tools (most "home spun").

State of the Art:

Commercial supply chain tools exist to meet this need. Some jurisdictions have limited programs, but at a very basic level. COTS inventory programs continue to increase capabilities, interoperability, and flexibility. Many programs share data across the Web and provide collaborative inventory decision making.

Technology Limitations and Barriers:

Technology is not a barrier – many similar packages exist in industry. However, the integration of a variety of different packages chosen by different responder organizations would be a significant problem.

Gap Fillers:

Commercial supply chain software could be adapted on a decentralized basis to meet this need, with the proviso that it interface with the LIS so that supply status be more broadly visible to incident commanders. Additionally, via a 3PL provider, commercial inventories could be made

visible to responders in times of crisis for needs to be met locally by rapid purchase. The inventory management software needs to be cognizant of location of inventory as it moves (in space and across jurisdictional boundaries), especially if interim supply depots are created. For this reason the most sensible arrangement would be to have the inventory management system serve as a modular element within the LIS.

LS.4 – Mortuary Affairs Management. *The ability of responders to recover remains and make forensic identification of victims of CBRNE incidents.* Recent history has made responders conscious of the magnitude and sensitivity of recovery tasks.

Goals:

- An information system that can match DNA of many recovered fragments to multiple DNA samples of victims or relatives (sometimes each in the 1,000s).
- Provide temporary morgues on site.

Current Capabilities:

Existing capabilities vary across localities but are geared for standard forensic work. The New York City (World Trade Center) and Oklahoma City incidents demonstrate a need for procedures and information tools to be linked. Standard forensic DNA tools are designed for comparing one sample to a few possibilities. The need to match multiple samples to vast populations increases complexity. Evidence rules normally require medical examiner notation of all bodies or parts recovered. Thus delays occur in massive events. Two temporary morgues (equipment caches) currently exist in the U.S. Potential military assistance is extremely limited. The Army has only one active duty mortuary affairs company (54th Quartermaster) without laboratory capabilities for scientific identification.

State of the Art:

The following technologies are available:

- PDA-based scanning technology for inventory and segregation.
- Forensic DNA typing technologies.
- GPS for site marking and discovery.
- Use of animals and limited mechanical sensors for finding body parts.

Technology Limitations and Barriers:

The primary technology challenge is making the identification, not tracking it. Automated techniques for sensing and finding body parts have not been a real focus of investigation. The high level of background contamination on the site of an explosion, fire, or building collapse poses difficulties for detection technology. DNA matching technologies take too long because of the need for amplification. Also, current technologies require expert personnel, so the need for training of personnel and providing experts rapidly to incidents is a problem.

Gap Fillers:

Several initiatives are worth exploring:

- Robotic system with appropriate sensors (artificial nose) for location of body parts.
- Automated support for geospatial and forensic record keeping of remains.
- More rapid techniques for matching DNA in the hundreds to thousands context.

LS.5 – Lightweight, Long-Lived Power Sources. *Longer-lasting, lighter weight, shorter recharge, easy-to-manage batteries.* Batteries are expensive and consumed at a rapid rate by all categories of responders. Types of batteries are as varied as the systems they support. Shelf life and cost prohibit the warehousing of all battery requirements in ample quantities to support incidents. Weight and space prohibit the individual from carrying a supply of batteries to last for continual support during incidents. Standardization of equipment and batteries would be desirable but seems unlikely to happen soon given the large installed base.

Battery sustainment is a critical issue for interoperability.

Goals:

- Responder safety and effectiveness in emergencies that may require extended presence in the area.
- Rapid resupply with reduced logistics tail (supply and maintenance).
- Alternative power sources.
- Minimum 24 hour battery.
  - Reduce recharge time to under 15 minutes.
  - Reduce size and weight to absolute minimum for various categories of batteries.
  - Chip that tells the logistics system that batteries are running low.

Current Capabilities:

- Responders find that batteries limit their ability to operate equipment, even short of a full 8 hour shift.
- Batteries often fail without notice.
- Responders view batteries as unreliable, heavy, and large, with long and unpredictable recharge times.
- Gel cells and solar cells are used for communications and repeater systems, but are limited by weight.
- Generators carried by responder equipment are not geared for servicing individual responder equipment.

State of the Art:

The same issues faced by responders are receiving the attention from military leadership with specific programs and funding.

- A DoD program (STO IV LG 2003.01) is focusing on portable and mobile power for the Army's "Objective Force." This program is a 3 year effort at $20M designed to address lithium polymer technology.
- CECOM is also working with throw-away lithium battery technology, rapid charging technology (to reduce recharge times by 50 percent), metal-air battery technology, and integration of power distribution into clothing and equipment.

Exotic future power sources include novel electrochemistries, portable fuel cells and fluid electrolyte cells that are recharged by exchanging the electrolyte rather than being electrically recharged within the battery.

In general, however, the main driver for improvement in batteries has been the commercial market (cell phones, laptop computers, etc.). Except for very specialized purposes, this seems likely to continue to be the case.

Technology Limitations and Barriers:

The CECOM programs face problems in working with the market to guarantee the volume required to have commercial partners invest in the technologies. There is an inherent danger in attempting to standardizing power sources for future equipment; standardization inevitably has the character of a least common denominator, restricting performance and limiting innovation.

Cost is crucial. The cost for some future battery source meeting the specified goals may run the cost up to three times the current price.

Because economies of scale dictate that responders use battery technology that is commercially available, there is little possibility of economically producing specific developmental items for responder use.

Gap Fillers:

While the perfect world would at least standardize the equipment used by responders, legacy equipment would prevent this for some time even if standardization for new equipment were to begin today. Battery sustainment should be a critical concern when purchasing new equipment or upgrading. Additionally, large organizations should manage battery sustainment as a critical

item and seek contracts for rapid resupply during major incidents.

As communication capability begins to perfuse the responder community (for example via the personnel status tracker in UIC.1 (*Point Location and Identification*)), consideration should be given to automatic reporting of battery status to allow improved management of battery replacement.

DHS should ensure that both DoD and commercial battery developers are aware of responder power source requirements and that these requirements are factored into DoD R&D projects and acquisition requirements. However, the most likely scenario is that responders will benefit from advances in cell phone and laptop batteries.

LS.6 – Transportation Optimization. *The ability to have assured delivery of mission critical personnel and goods.* Transportation in support of an incident is often in direct competition for the same routes as emergency equipment (and evacuation). Sustainment is limited by scarce routes, assets, size and capacity of vehicles under degraded road conditions, and scheduling. Transportation planning, scheduling, routing, and mode determination are issues that require optimization and risk avoidance. Often the mix of commercial contractors, responder support, and other agency vehicles moving equipment and resupply creates transportation chaos requiring intervention on the part other responders (police) who may not be fully aware of the logistics situation or priorities.

Goals:

- *Local* – monitoring traffic patterns and restrictions, location of transportation bottlenecks and assets, all in near real-time.
- *Non-local* – Fed Ex, UPS and military long-haul transport; have plans in place to follow-through with local representatives of companies, or through digital communication.
- Personnel coordination with military transports.
- Secure, timely capabilities for command and control and rerouting.

Current Capabilities:

- Responders are conscious of imperfect integration between federal and local transportation resources, across local jurisdictions, and between public and private sector transportation authorities and providers.
- Emergency managers currently rely on commercial carriers, military transport, or contracts with local bus system operators.

State of the Art:

- Commercial software exists that can assist in route and carrier scheduling and selection so long as information on degraded networks is provided.
- Establishing emergency access routes for transportation bottlenecks and plans is addressed by large jurisdictions.
- Some cameras exist in large areas that provide traffic monitoring and permit changing traffic light patterns to optimize flow on command.
- Sensors on vehicles in traffic could automatically report positions and speeds to a central facility (assuming communications are available).

Technology Limitations and Barriers:

Technology exists to provide real-time monitoring of transportation assets. However, the costs are considered prohibitive. Equipping every vehicle on the road and providing visual monitoring of all routes is regarded as impossible by responders today. Another major problem is the conflict of responder needs with evacuation of citizens from danger zones. The confusion in New York City on September 11th is a perfect example. Here logistics needs to be facilitated by capabilities in Chapter VI (EMPP) and Chapter V (R&R).

Gap Fillers:

Some COTS products exist that could be made available to plan, optimize, and execute logistics

transportation assets. For example, i2 Technologies recently fielded a lightweight application with basic map visualizations to the Army's 7th Transportation Command for port clearance and sustainment delivery. Providing a basic capability for planning and execution would be a start. This could be accomplished within a year at a cost of approximately $2M. Technologists quickly imagined many systems concepts that could relatively inexpensively provide information on the status of the road network. UAVs or aerostats could provide inexpensive traffic flow information in conjunction with other emergency missions such as communications relay. If communications bandwidth is available, communicating tags on vehicles hold substantial promise of providing adequate near-real-time information. (If the cell phone system is working, one could imagine that a small reprogramming of the OnStar and similar systems in cars could be used to automatically report information on traffic speeds and bottlenecks. Such an emergency mode could be required on cars and trucks equipped with similar GPS systems in the future.)

LS.7 – Assessment of Safe Air, Sea and Ground Bases of Operations (Supply Depots). *The ability to assess the safety, security, accessibility and capacity of potential bases of operations (supply depots).* During an incident, logistics responders often need to establish temporary locations to marshal personnel and supplies and to operate support bases. Route considerations, space, buildings, and security are factors that must be considered, while locating the operation as closely as possible to the incident. In some cases, more than one site may be required. The assessment must be rapid and accurate to ensure that the response is not delayed or impeded.

Goals:

- Real-time satellite imagery (GIS), sensors of storage locations and adjacent routes.
- Template of requirements for basing – nature of materials, resulting base requirements.
- Database of locations which could be used for support bases; updated regularly.
- Consideration of security (to include marine, temporary structures).
- Rapid and accurate re-assessment during an incident to avoid delays in response.

Current Capabilities:

Most localities have identified areas for use, but not a database of areas. Technology that could help determine safety of the areas (GIS/sensors) is not available and/or very expensive. Local knowledge is applicable but interaction of availability with detailed requirements is not currently facilitated.

State of the Art:

Technologists noted programs exist, that if integrated with LS.1, could assist logistics responders:

- UAVs, satellite photography (remote imaging/sensing).
- National databases for ports and airfields (NGA) with integration into decision support tools (Transportation Command (TRANSCOM) and DARPA both have created limited products).
- *CECOM* – Single Integrated Ground Picture (SIG-P).
- Military Traffic Management Command (MTMC) route databases.
- Intelligent Roadway and Railway Information System (IRRIS).

Technology Limitations and Barriers:

The main limitations to full capability in this area are in the area of resources. To a lesser extent, there are issues with how best to integrate heterogeneous sensors (a central concern in Chapter III (DIDA)). Problems of knowledge management, representation, and optimization would need to be worked through but these are

not particularly difficult problems. Finally, information collaboration across jurisdictions would be a practical issue. However, none of these is considered a technology limitation.

Gap Fillers:

The technologists determined that this issue can be facilitated by adapting existing government products for civilian use. The concept would be to permit access to systems over the Web which provide collaborative viewing of the operational picture. Integrating the Web-based Joint Theater Logistics collaborative mapping tools into the LIS can provide planning and real-time execution management of depots. This effort would take two years and possibility up to $15M to field the capability for use by responders nationally.

Logistics Support Response Technology Objectives (LSrto)

LSrto.1 – Integrated Logistics Information System (ILIS). This Responder Technology Objective is designed to improve capabilities for LS.2 (*Automatic Generation and Assessment of Supply Requirements*), LS.3 (*Inventory Management*), LS.6 (*Transportation Optimization*), and LS.7 (*Assessment of Safe Air, Sea and Ground Bases of Operations*), in addition to LS.1 (*Logistics Information System*).

Objectives:

Develop an integrated yet evolutionary Integrated Logistics Information System capable of connecting all echelons of command (including regional and national) and all types of suppliers and other logistics nodes. The functions of this information system include planning and launching the appropriate initial logistics response to support emergency response to disasters, tracking inventories and items in transit (across jurisdictions), projecting needs for consumables and other support items including transportation, providing information and decision support for transportation optimization, and providing information relevant to the rapid assessment of safe bases of operation. The information system should use communication links provided in Chapter IV (UIC). It must be based on an open architecture that allows software from different vendors to interoperate, and it must provide basic interfaces (Web-based and call-centers) that allow some level of service to and integration with departments lacking modern logistics systems.

Payoffs:

Such an integrated logistics information system is the only feasible way to ensure that the decentralized and diverse character of responder organizations does not remain a significant impediment to mission support in the difficult context of the limited resources available for a response to catastrophic terrorism and the significant physical obstacles that would attend such a response.

Challenges:

There are no severe technical challenges in providing the individual components of a logistics information system that would provide significant improvements to capability. Careful system design should allow multilevel processes, some advanced planning, and additional human effort to provide adequate capability even if the most advanced capabilities outlined by technologists (automatic domain-bridging and wide-area tags that cannot be jammed) are in fact not achieved. However, very significant challenges do exist, including: software integration on the scale required, providing for the needed level of openness to the variety of user interfaces required while also providing for continual evolutionary improvement. A further challenge will be enticing both software vendors and responder departments to participate in the development and technology transition processes.

Milestones/Metrics:

FY2004: Develop the basic architecture for the LIS and the mechanisms by which the development will be carried forward. (In other words determine the boundaries and ownership of and supervisory structure for centrally-provided utilities and interfaces and the procedures by which modules that will be owned and used by responder units will be certified and maintained.) Begin the short-term initiatives listed as gap

fillers under LS.1 and the evaluation of the longer term gap fillers (next generation tracking and automated domain bridging).

FY2005: Provide an initial demonstration test-bed including appropriate initial simulations and scenarios that will allow evaluation of off-the-shelf software components. Establish a roadmap of milestones for incremental capability rollout. Complete the evaluation of longer-term initiatives and establish a plan of action for them.

FY2006: Establish an initial operating capability for central services; establish two regional operational testbeds.

FY2007: Establish a third regional operational testbed.

FY2008: Initial National Operational Capability for the LIS.

LSrto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
ILIS	$9	$21	$27	$32	$40	**$129**

LSrto.2 Many-to-Many DNA Matching of Body Parts

Objectives:

Develop the capability to recover, track, and identify using DNA comparisons of bodily remains from mass casualty events.

Payoffs:

Such a capability would ease the uncertainty and suffering of relatives and also aid in the forensic reconstruction of mass casualty events.

Challenges:

The rapid development of novel DNA sequencing technologies provides the means for achieving this capability but it also means that the process of choosing a technological approach will be uncertain.

Milestones/Metrics:

FY2004: Review technologies for locating and recovering remains and possible approaches to rapid DNA comparison. Issue an RFP for elaboration of technical approaches and proof of concepts.

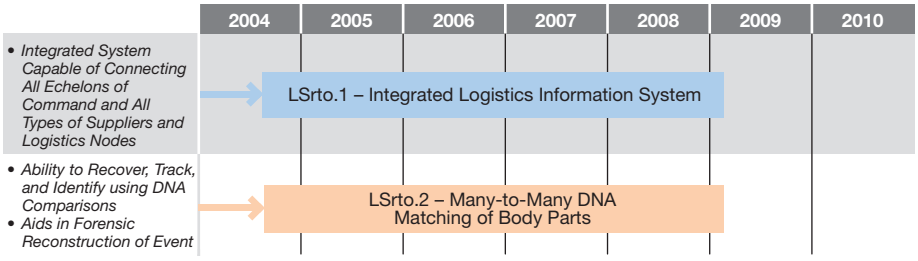
FY2005-2006: Choose a maximum of three recovery and three identification technologies for further development; issue appropriate RFPs and fund winners.

FY2007: Field prototype systems; conduct demonstrations.

FY2008: Develop operational systems for fielding in FY2009.

LSrto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
DNA Matching	$3	$6	$10	$10	$10	**$39**



Logistics Support Technology Roadmap

Chapter X

Crisis Evaluation and Management (CE)

Chapter Chair: Hal Kempfer
Chapter Coordinator: Michelle Royal

Definition

Crisis Evaluation and Management (CE) is the ability to enforce the law and protect public safety by anticipating, preventing, reducing and/or removing a threat or act of terrorism including disabling terrorists and threat devices.

Operational Environments

This NTRO is focused on the five operational environments represented by threat: chemical, biological, radiological, nuclear, or high-explosive/incendiary effects of an event (*i.e.,* CBRNE).

Needed Functional Capabilities and Priorities

Responders and technologists considered a set of six functional capabilities required to function in the operational context described above. These capabilities are presented below in order of descending priority:

- Identifying, Locating, Disarming and Seizing Perpetrator(s)
- Tactical Threat Assessment
- Disposing of CBRNE Devices
- Initiating Crisis Management Process
- Perimeter Security
- Media Management and Accommodation

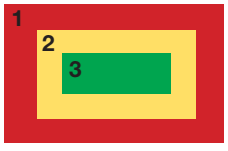
Overall State of Technology for Crisis Evaluation and Management

Capabilities providing intelligence, surveillance, and reconnaissance (ISR) are critical to crisis evaluation and management capabilities. Responders generally lack high-technology ISR tools integrated in such as way as to cross jurisdictional and disciplinary lines. Many systems used in the special operations, military and intelligence communities are not widely used by responders. In some cases, "low-density high-impact" items such as millimeter wave imaging technology or adapted remote-controlled fiber optically-guided vehicles could be decisive in providing real-time intelligence needed for crisis evaluation and management.

The matrix below shows that technology is available today to increase capability in most of the lower-priority functional capabilities. The chart

Crisis Evaluation and Management

Functional Capabilities	Operational Environments: Chemical	Biological	Radiological	Nuclear	High Explosive/ Incendiary
1. Identifying, Locating, Disarming, and Seizing Perpetrator	2	2	2	2	2
2. Tactical Threat Assessment	2	1	2	2	2
3. Disposing of CBRNE Devices	3	2	3	3	3
4. Initiating Crisis Management Process	3	3	3	3	3
5. Perimeter Security	3	3	3	3	3
6. Media Management and Accommodation	3	3	3	3	3



1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

indicates, however, that in the higher-priority functional capabilities, there are still moderate technology challenges to increasing capabilities. It will be important to focus on these challenges, especially in tactical threat assessment in the biological environment, where responders indicated that virtually no capability exists today.

CE.1 – Identifying, Locating, Disarming and Seizing Perpetrator(s). *The ability to neutralize and then apprehend the perpetrator(s).*

Goals:

- Ability to neutralize and take custody of the perpetrator(s), eliminate the threat without hindering the ability to acquire more information and evidence, understand the threat, etc.
- Safety for responders, hostages, and if possible perpetrators.
- The technology of the responders should exceed the technology of the perpetrators.

Current Capabilities:

Responders divided the capabilities of CE.1 into two main areas; 1) identifying and locating perpetrators, and 2) disarming and seizing perpetrators. The first area is more ISR-intensive; the second area more focused on tactical operations. The crucial technologies for both of these areas are: ISR systems, non-lethal weapons, and sensors and tracking. Safety for responders and the public is a constant theme. Technological superiority of public safety officials over perpetrators is implied or assumed (although during workshops, perpetrator technology was occasionally brought up for benchmark discussion and to challenge assumptions).

Initially, responders need to be able to identify a suspect or perpetrator quickly through both information sharing systems and technologies to physically identify perpetrators. There are a variety of means available today to do this if the suspect's identity information is already archived. For non-intrusive identification, facial recognition (and voice recognition) technology and software has been used for law enforcement applications as well as for counter-terrorism at special events (*e.g.,* the 2003 Super Bowl). Details on this are further explained in CE.5 *(Perimeter Security)*.

COTS technologies for facial and body recognition are available today for identification of perpetrators in the field. Some advanced applications of this technology have been developed in Las Vegas casinos. Voice recognition software with advanced wireless technology is seen as a way to do biometric identification in the field through voice print analysis technology. Technologically, this has far greater potential today due to recent advances in wireless telecommunications and opportunities for better exploiting the standard technique of field interviews.

One technology requirement discussed by responders is the need to "see through walls." Infrared "flashlights" or portable camera systems are commercially available that can provide images from inside buildings and vehicles to determine "hotspots," such as people, lamps, etc. At border crossings, infrared imaging of containers and vehicles is a common practice used by U.S. Immigration and Customs Enforcement (ICE). Millimeter wave cameras are also used for "remote frisking" to detect weapons or drugs carried by persons.

Non-intrusive tracking measures include surveillance technologies such as optical sensors and software that can discriminate between colors, shapes, movement and background. Law enforcement helicopters use these technologies to follow moving vehicles in heavy urban traffic.

For physically capturing and disarming perpetrators, there are a variety of capabilities available, to include lethal force, and "non-lethal" capabilities. non-lethal technologies include bean-bag projectiles and rubber bullets, flash-bangs, sticky foam, HERF (high energy radio frequency including high power microwave or HPM weapons), robotics, tasers, net guns, microwave vehicle stopping, NIJ's ring airfoil projectile (RAP), and advanced weapons being developed at the U.S. Army's Picatinny Arsenal and Rome Labs.

Disabling perpetrators wired with remote or suicide explosives presents a challenge against which responders have no capability. Responders need a technical means to block or neutralize the frequencies of a remote detonating transmitter without detonating the device itself. Disarming and seizing such a perpetrator puts responders and the public at substantial risk; the presence of chem/bio or radiological agents presents a variety of additional technical challenges.

State of the Art:

Programs such as the Regional Information Sharing System Network (RISSNET), Open Source Information System (OSIS), Law Enforcement Online (LEO) and Joint Regional Information Exchange System (JRIES) show dramatic promise for sharing critical threat intelligence, or criminal or perpetrator identification and location. However, these systems are not fully integrated. Integrating these systems would appear "low-hanging fruit" that could result in large returns on investment. With OSIS now being managed under the INTELINK office, the capability exists to more quickly sanitize and then further tie together classified federal intelligence into timely bulletins, warnings or database information for unclassified dissemination to state and local authorities.

Database information on the perpetrator is essential, along with the ability of responders to quickly query online databases. RISSNET is designed to share law enforcement information across municipal and state boundaries, and tie state and local law enforcement in with federal law enforcement agencies. RISSNET currently provides valuable information on potential or actual perpetrators of terrorism to support active investigations, although much of the RISSNET data is still related to drug investigations.

The FBI's Law Enforcement Online (LEO) system was originally started as an alternative to RISSNET, but is now is integrated with it. LEO has a multitude of applications and information sharing tools. RISSNET has six networked regional centers that share criminal intelligence and information, to include perpetrator data, and provides a systems interface to coordinate efforts against criminals nationwide. LEO is available to state and local law enforcement, but is a U.S. Department of Justice sponsored system managed by the FBI.

Non-lethal technologies, whether against persons or vehicles, are not fully mature, and probably require several years' development for full utility. Tasers and the ring airfoil projectile hold promise for wider application in the NTRO, and could be critical gap fillers until more robust technologies come online. The air taser is a very popular non-lethal weapon that uses projectile probes connected by wire with a power source to deliver a large high voltage, low amperage charge to the target. It is widely used in law enforcement, corrections, security work and for self-protection. The drawback is that there is no technical means at the time to make the probe or round self-contained; it must be connected to the main gun by wires. This dramatically limits range and utility, with maximum range of 21 feet, and very limited ability to quickly engage other targets.

Lasers are currently used for aiming of ballistic rounds (and illegally used by criminals for flash blindness of enforcement personnel or opponents), but may be used in the future as a carrier of disruptive effects such as tetanization to disrupt muscle function. The technology to this does not exist yet, it is mostly theoretical and several years off by most estimates.

While not technology *per se*, there is a general responder shortfall in working with technology, particularly for analytical purposes. Identifying and locating perpetrators and developing threat assessments are primarily intelligence functions tied to investigations, but not solely investigative. Personnel such as Criminal Intelligence Analysts (with the State of California), or analysts with DHS and the FBI are not trained with technology, software and techniques commensurate to their other intelligence community counterparts. The ability to assess a transnational criminal enterprise, or one that simply supports terrorism, and then define its *modis operandi*, infrastructure,

key players and their roles, etc. is different from the training for standard crime analysis.

Technology Limitations and Barriers:

A significant barrier is the problem of systems developed along "stovepiped" bureaucratic lines, which prevents information sharing. Federal bureaucracies (and state and local agencies) have been wedded to their own in-house systems as the backbone of their information management program. The FBI uses FBINET, the DEA uses NADDIS or FIREBIRD, ICE uses TECS II, and so on throughout the government. Shared information systems such as RISSNET, JRIES and LEO are often viewed as secondary and less useful, except for some state and local enforcement agencies that have adopted them as their primary law enforcement sensitive database.

LEO, RISSNET, OSIS, JRIES and OpenNET are not fully integrated. Looking at their systems backbones and operating software, there does not appear to be a clear technological limitation from further or complete integration of these systems.

For responders, information or intelligence sharing is a key part of identifying perpetrators, but security of sensitive case information has been a primary limitation to sharing perpetrator data. Workshop participants highlighted the Drug Enforcement Administration's (DEA) National Drug Pointer Index (NDPIX) system that allows data queries on various types of information fields such as names, numbers, addresses, dates, etc. While allowing "cross pollination" between investigators, it only allows sharing of as much information as the inputting investigator, or analyst wishes to reveal. When a query results in a 'hit,' contact information for the case agent or analyst is provided. This linkage process allows wide dissemination of key data components to other law enforcement agencies while protecting sensitive data surrounding persons, places, numbers or things involved with ongoing or sensitive investigations.

There are significant technological barriers to developing systems to stop a perpetrator threatening to detonate a WMD (to include high-yield explosives). With current non-lethal technology, there is no assured method of achieving "instant paralyzation" without killing the perpetrator. The only truly fail-safe means to stop a perpetrator was referenced by the term "head shot," meaning a ballistic projectile being fired into the perpetrators brain causing instant cessation of cognitive and sensory capabilities, to include motor function. By the same token, even this solution was potentially flawed due to the terrorist perpetrator only having to build a simple "dead-man's switch," which triggers the device when pressure is removed. Examples of this are found in Israel with suicide bombers.

When disarming the perpetrator, there was concern about interference of RF (radio frequency) signals from portable communication devices used by responders, with mention that as little as five watts could trigger a standard high explosive device. All capabilities developed for responders should heed this risk, especially those developed to disable perpetrators.

Gap Fillers:

There was discussion by responders of using a "stepladder approach," building symmetrically on capability sets as they were developed or fielded. This approach includes establishing an urban testbed of new concepts and technologies; figuring out what works and what does not in a shorter time period.

A near-term gap filler is to leverage the explosion of mobile information or telecommunications infrastructure. The ability to collect and send information to and from the field has grown exponentially over the last few years, and this provides tremendous advantages for responders in how they can identify and locate a perpetrator. When combined with technologies such as facial, body and voice recognition, or even biometrics such as electronic fingerprinting, there is an ability to rapidly identify perpetrators, and then front-load critical intelligence on them to facilitate accelerated or safer apprehension. Examples include merged technologies of PDAs (personal

digital assistants) that can store images, cell phones with cameras, Blackberry systems used for paging and email usage during a crisis.

While known sensor and biometric technology appears far less than 100% accurate or foolproof, collectively they appear to have great deterrence value and redundancy that greatly minimizes or mitigates the chance of perpetrator or device remaining unidentified if "sensed." Technologists and responders discussed the establishment of some sort of fixed or semi-fixed system of sensors in critical places, and much of this seemed centered on high profile targets like sports venues or theme parks.

Current practice at many large public events is to physically check personal identification and search any bags, carriages, etc. upon entering the facilities or venues. Technological means exists to conduct multiple biometric and sensor scans using existing systems of persons and personal gear. This would provide an automated tool to flag anomalous characteristics for further inquiry or search. While there are still substantial improvements in these systems to be done, this capability has the potential for screening more people faster, while exhibiting a strong deterrent to those trying to do something unlawful. An 80%, or even 50%, accuracy rate for facial recognition, combined with a digital fingerprint match, voiceprint match, and an array of millimeter wave and "sniffer" sensors, would appear to be a potent gap filler.

There is nothing more reliable or realistic than the current low-tech approaches such as spike strips to stop vehicles. For apprehending or stopping persons, it appears that short term gap fillers are confined to tasers, air tasers (with their extremely limited range) and possibly advanced fielding of the new ring foil projectile being developed by NIJ (see CE.5 (*Perimeter Security*)).

CE.2 – Tactical Threat Assessment. *The ability to assess threats inside buildings (i.e., seeing through walls), identify individuals and objects that are at risk, and have awareness of perpetrators' actions, position, and status of devices and weapons.*

Goals:

- Rapid (within minutes) risk, hazard, and situational size-up.
- Ability to differentiate perpetrators from the other people (hostages, victims, bystanders and responders).
- All-in-one integrated suite that also tells you what you are dealing with (a "reach" goal).

Current Capabilities:

There is very limited capability for tactical threat assessment in reference to meeting these goals, with almost no available capability for biological threats. There are current technologies that can be applied such as infrared imaging, acoustic detectors and processors, radar motion detectors, and optical motion detection.

State of the Art:

Acoustic technology that can penetrate solid surfaces exists, and DoD has done considerable work in this area. "Ping" technology was referenced by responders and technologists as a tool for identifying hidden weapons or devices in tactical threat assessment. "Multi-ping" technology uses variations in the local acoustic environment exploited by target classification algorithms. This falls under the category of broadband active acoustic signal processing, particularly the area of nontraditional homing.

Imaging millimeter wave sensors can be used with some measure of stand-off to see through the walls of buildings. It is essentially microwave flooding that can provide a sense of where walls and flooring are, and then provide movement patterns by taking the differences in the baseline with the current images. The limitation is that it cannot see completely through the building and does not provide a high resolution motion video picture, but it can tell if there is movement in the front rooms of the building and where that movement is located. Special operations and counterintelligence units have been using this technology for some years, and the equipment is

specially manufactured and obtained through intelligence channels.

In addition, a system using millimeter wave sensing is completely contained within van that can drive up and down parking lots or other car locations and "look into" vehicles to identify compartments. This is a significant improvement over earlier versions that had a backscatter issue requiring a hard backing on the target. The new system requires no such backing and is completely self-contained.

Another technological approach used for tactical assessment of building interiors is small, remote controlled vehicles with a fiber optic link and special sound dampening rubber wheels. With access to an air shaft or other avenue of approach, these vehicles can gain surreptitious entry for observation and audio collection on the targets. Normally, the system is outfitted with infrared imaging capability.

Along with the more advanced means, there is also standard equipment such as fiber optic cameras for peering under doors or around corners, along with less hi-tech mirrors. These fiber optic systems can be remotely controlled over short distances to twist or turn in a particular direction to aid movement or observation. There are also a myriad of miniature cameras and listening devices that can be clandestinely emplaced, but this requires very close proximity to the target in order to do so. There are also parabolic dish devices for listening to conversations over extended distances, and many different ways that listening or camera devices can be secreted into apparel, eyeglasses, luggage, doorknobs, "pole cams," "tree cams," or other common items.

DARPA is working on projects that will equip small ISR (intelligence, surveillance and reconnaissance) systems like UAVs (unmanned aerial vehicles) to detect perpetrators, and use sensor systems to detect chemical, radiological and biological weapons. Obviously, these could be easily adapted for emplacement on a remotely controlled tactical ground vehicle, with space and weight limitations being a consideration.

The Department of Homeland Security is starting test flights at Fort Huachuca and Gila Bend in Arizona on unmanned aerial vehicles, building on the lessons learned and adapted applications developed in Afghanistan and Iraq. UAVs bring some distinct advantages such as a loiter time of 4-50 hours, far longer than manned aircraft can sustain, and fly at a high enough altitude to be virtually undetectable by noise. A UAV or drone being used for this purpose outfitted with cameras and sensors can cost between $1.5 to $4 million, which compares very favorably to costs incurred from helicopter or other manned aerial surveillance options with similar capabilities.

Systems that archive building plans can afford rapid access to blueprints, floorplans, and even photographs of building interiors to assist with tactical assessment. Currently, most large buildings and facilities submit plans to the fire department, and tall buildings are required to have blueprints on hand in the lobby for responders to reference as needed in cases of emergency. Software exists that allows 3-D manipulation of these plans. This facilitates the ability of a responder to "see" into a building.

Technology Limitations and Barriers:

Portability of these technologies is a major technological barrier to meeting the goals of this functional capability. In addition, stand-off sensor systems that use millimeter wave, infrared, or other radar technologies will continue to face technological challenges penetrating thick walls sufficiently, and yielding enough detail, to meet the accuracy demands of sensitive, dangerous tactical operations involving armed perpetrators and possibly hostages.

Gap Fillers:

A key gap filler is to digitize building and facility data for rapid access and 3-D manipulation by tactical responders. This should build on both technologies and policies that automate the collection, digitization, and compilation of information gained as various members of the public safety community visit and inspect a given building. For example, fire inspectors,

health inspectors, building code inspectors, municipal licensing authorities, police officers, etc., as they inspect a building in the course of their duties, could provide data to an automated information system, such as how many people work in an office, daily operation patterns, or a potential vulnerability of a particular location. This information could to be tied in with the building plans or layout to provide responders and tactical commanders a far more complete picture of the building and what is likely inside it. Moreover, it would provide a foundation for an open architecture for augmentation by advanced "see through wall" sensor systems as they become available and are perfected.

Another near-term gap filler is to develop a technology bridge between public and private sector closed circuit television (CCTV) and other remote sensor systems. This sort of public-private cooperation has been done successfully in other spheres, to include utility and information sharing. The administrative burdens and technological challenges would be minimal.

CE.3 – Disposing of CBRNE Devices. *The ability to disable, render safe, contain, handle, transport, and dispose or destroy of contaminated threat devices, including contaminated explosive ordnance disposal.*

Goals:

- Containment or otherwise management of "excessive" amounts of explosives.
- Accomplishing this functional objective safely while preserving evidence or sources of intelligence, and not exacerbating the situation.
- Ability to render safe the location where the device was built/assembled/grown, if the location also poses a threat.

Current Capabilities:

Most large jurisdictions, especially the federal agencies, have the capability to dispose of chemical devices. A marginal capability exists to dispose of high explosive devices, usually limited in cases of "excessively" large amounts of explosives (the challenge is handling the mass of explosives, rather than the type of explosive). No capability exists at local levels to dispose of a biological, radiological, or nuclear devices sufficient to meet the goals, although responders recognize these capabilities exist at the federal level.

State of the Art:

Workshop participants felt that much of the state of the art for this capability resides with the military and federal agencies. For example, if a jurisdiction faced the problem of disposing of a radiological device, they would not attempt to do so on their own. The Department of Energy Nuclear Emergency Response Teams (NEST) teams are designed and equipped for this mission and would be called in. Similarly for biologicals, the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) has disposal capability.

For the responder community, there are some total containment vessels that will contain a moderately-sized explosive device (2-5 lbs) which are available to responders. In addition, a tent device is being developed in Canada which disperses foam that degrades biological agents.

Technology Limitations and Barriers:

Limitations and barriers for *Disposing of CBRNE Devices* are similar to those for decontamination. There is always a question of "how clean is clean." The device, and all trace particles from that device, needs to be disposed of with a level of surety that will placate both responders and the public. Cost is also represented as a technological barrier here because the large price tag associated with some of these items is prohibitive for all but the largest jurisdictions.

Gap Fillers:

A primary concern of the responders is development of technologies to aid in the disposal of biological devices. The technologists also felt that this operational environment presented the biggest challenge for technology development to meet the responders' needs. This capability is related to the development of sensors (see

Chapter III (DIDA) which are needed to determine the composition of the device, and therefore the proper disposal means. Responders commented that they have to way of reliably containing an unknown threat.

CE.4 – Initiating Crisis Management Process.

The ability to initiate functions, systems, and technologies to support decision-making, course-of-action determination, and subsequent incident action plans.

Goals:

- Timely, automated notification of other agencies, disciplines, and levels of government with functional responsibilities.
- Automated activation of Memorandums of Understanding (MOUs) and Mutual Aid Agreements, etc.

Current Capabilities:

Responders do not have this functional capability today in an automated system. Activation of crisis management processes is still a manual, chaotic process.

State of the Art:

Responders and technologists agreed that the technology exists today to enable this functional capability. It is only a matter of integration and implementation, beginning with a policy-level decision to do so. There are several examples of technology approaches that could be integrated.

California's Response Information Management System (RIMS) is a statewide computer system used to coordinate and manage the state's response to disasters and emergencies. It is Internet based, and was developed by the California Office of Emergency Services (OES) in 1995. Today it has over 2000 internal and external clients, and is available to all cities, special districts and state agencies within California that have a computer access through the Internet, and is controlled through IDs and passwords.

In San Diego, as well as other cities, there is the "find me, follow me" system for automated paging and calling of key emergency response personnel or emergency managers. The system will tell those on duty who is available and how far out they are, and it is event driven. It keeps on calling or paging someone until it gets a response that they have been found and the message delivered.

For seismic events in California, the state developed EDIS (Emergency Digital Information System) following the Loma Prieta earthquake in the San Francisco Bay Area in 1989. However, this has since grown considerably, and is a combination Website, newsier and 24 hour broadcast service. Authorized agencies can release text, pictures and sounds over EDIS using their own existing networks, and the news media and public have access to the latest EDIS information over the Internet, via digital radio broadcasts, on their pagers, and by email.

EDIS is designed to be disaster-resistant, with a sophisticated satellite distribution network constantly updating "mirrored" EDIS servers in selected newsrooms and networked facilities around the state. Even when public networks are clogged after a disaster, EDIS information will be available statewide.

Technology Limitations and Barriers:

The technologies exist today to deliver this capability. Cost and political will are the biggest barriers. Systems that rely on cellular or other telecommunications networks will encounter the same technological challenges that are present today (*e.g.,* bandwidth availability, cell disruption or overloading, nodal failure or destruction, etc.).

Gap Fillers:

At the municipal or regional level, the main gap filler would be the development of a standard system such as the "find me follow me" system that San Diego has put in place. For automated triggering of mutual aid and memorandums of agreement, the Washington metropolitan system established by MITRE would appear to be a benchmark for expansion and adaptation.

CE.5 – Perimeter Security. *The ability to control individuals, crowds, and vehicles, to prevent public disorder or endangerment from the threat (i.e., keeping public out of the blast radius, keeping the public from snipers or hostage-takers, etc.), and to keep public citizens and vehicles from interfering with efforts to manage and reduce the threat.*

Goals:

- Public safety – keep the public out of the danger zone.
- Extend and control security perimeter and zone far enough out so that response personnel and staging activity can operate unhindered by the public.
- Ensure that only authorized credentialed individuals are within the perimeter. This also would include authorization of equipment entering perimeter/staging area.

Current Capabilities:

Responders have a marginal capability to meet these goals today, hindered mainly by the ability to ensure authorized credentialed personnel within the perimeter. The technologies to achieve these goals exist today.

State of the Art:

Currently most emergency or consequence management locations, especially involving CBRNE, are sealed off manually using personnel and tape to keep intruders away. As the situation develops, physical barriers are put in place, and over time temporary fencing may be emplaced as well. For pre-existing facilities, such as amusement parks, major airports, shopping centers and casinos, there may be an existing CCTV system that can provide remote visual surveillance of the perimeter to augment "boots on the ground."

In major HAZMAT incidents, emergency responders have often had to man checkpoints and set up a perimeter with personnel keeping out intruders, or enforcing an evacuation of downwind areas. The same capability will probably be relied upon for a CBRNE incident.

For access control, there are a variety of technologies that can be applied to ensure only authorized personnel are allowed access to within the secured perimeter. This includes technology like bar codes, magnetic strips, passwords and so on. More advanced technology measures biometric data (*e.g.,* retina scanners, face recognition). Smart cards can also be applied to this capability, capturing personnel authorization as well as training proficiency and currency (see Chapter VI (EMPP)).

Responders were also concerned about tactical accounting of equipment into a control zone. One common technology used to account for this is to attach a tag with a bar code. More advanced technology involves attaching a remote transmitting device that can then be monitored remotely. GPS technology, similar to what is used with On-Star devices on automobiles, can send out the signal of where the equipment is at any given time.

Surveillance technology for monitoring a perimeter was deemed very important to responders, with great interest on CCTVs, motion detectors and unattended ground sensors. All of this technology exists, and the ability to establish a network using wireless networking has only recently become easily achievable.

Technology Limitations and Barriers:

The technologies are available in the near term to meet the goals of this functional capability.

For authorization verification, there are still problems with reading strip cards, especially in the field. Sometimes the magnetic strip loses its code, or the automated reader is otherwise unable to read the card. In a field environment with a fast-paced crisis or event, corrective action may not be immediately available. There is also the possibility of counterfeit cards being produced, and the sophistication of counterfeiters today makes this a serious threat. It is possible to embed anti-counterfeiting technology into the system, however. If cards are used, there would be a need for a lot of readers and reading stations, which would become manpower intensive, either

taking away from the available responders in order to manage this activity or requiring additional manpower dedicated to this activity. Furthermore, the technology of biometrics is not fool-proof, and both technologists and responders were aware of false positives and false negatives being a substantial problem.

Non-lethal force technology for perimeter control is a critical concern of responders. The current state of non-lethal technology deployed in the field is inadequate to address enforcement of perimeters without resorting to the threat or use of deadly force. The scenario of a little girl running away from a quarantine area comes to mind, with the implied ethical, legal and political questions of whether deadly force should be used, with the corresponding failure to stop her as risking the chance of a greater epidemic.

Non-lethal enforcement of quarantine operations is becoming more important. With major incidents, civil-military operations are more likely. In many cases, this will require military augmentation in the role of large-scale quarantine operations. Whereas technology exists to identify quarantine violators with substantial stand-off range depending on the perimeter, the ability to stop them from escape is primarily the threatened use of lethal force at present.

Gap Fillers:

There is technology being developed that allows the reader to scan the thumbprint of the person holding the card with the card, thus minimizing the chance of counterfeiting ID. Smart chip technology is also a readily available solution that can meet needs in this and other NTROs such as Medical Response, Emergency Management Preparation and Planning, etc.: anywhere where identification, location, and proficiency of personnel needs to be known by an incident commander.

CE.6 – Media Management and Accommodation. *The ability to manage and accommodate the media such that media personnel and equipment (e.g., vehicles, lights, recording/broadcasting, and communications equipment) does not give the perpetrator any tactical benefits from media exposure.*

Goals:

- Keep the media within the right places inside the appropriate perimeter, such that no sensitive tactical operations can be broadcast by the media.
- Provide enough access to the press to satisfy them to the extent that they do not try to thwart the above functions. This includes cooperation with the media to the extent possible without compromising the operation.

Current Capabilities:

Responders have this capability today.

State of the Art:

Responders felt that this capability is not technology enabled. Good relationships with the media result in the best outcomes for managing media personnel and equipment, as well as information flows.

Crisis Evaluation and Management Response Technology Objectives (CErto)

CErto.1 – Non-Lethal Safe Seizure of Perpetrators

Objectives:

Develop less-than-lethal technologies to instantly immobilize perpetrators with weapons or hostages, such that explosive devices or other weapons are not detonated, released, etc. This technology will not emit radio frequency or other signals that might set off an RF detonator.

Payoffs:

This will provide responders a way to take perpetrators into custody without relying on deadly force, or presenting a danger of detonating the perpetrator's weapon.

Challenges:

Some of the more exotic technologies, like HERF, are still in the R&D phase, and won't be

available for years. When they do become available, some of the less technical means currently available may quickly become obsolete.

Traditionally, identifying and seizing perpetrators has been focused on the professional knowledge and judgment of the agent or officer on the scene. Modern communications technology has been slowly eroding this traditional approach, and the technology being discussed here would erode that more.

Milestones/Metrics:

FY2005: Review the state of the art in non-lethal technology developments in the DoD and public safety community and assess the applicability of the technology to the goals in this NTRO. Develop concepts of operation and functional specifications for a suite of non-lethal tools.

FY2006: Select enabling technologies for the initial operational capability (Block 1) of the non-lethal suite of tools. Develop the architecture and Broad Area Announcement to begin development and integration of Block 1.

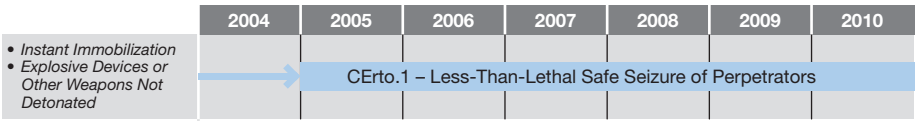
FY2007: Continue development of Block 1 suite. Begin commercialization process and planning for operational demonstration. Begin development testing of Block 1. Select enabling technologies for Block 2 capability.

FY2008: Conduct operational demonstration of Block 1 capability. Begin development of Block 2 suite of tools. Continue commercialization efforts.

FY2009-2010: Deploy Block 1 suite. Continue Development of Block 2. Conduct development testing of Block 2. Demonstrate Block 2 in an operational environment. Deploy Block 2.

CErto.1 – Budget in Millions

Thrust	2005	2006	2007	2008	2009	2010	Totals
Non-Lethal Suite of Tools	$5	$7.5	$8	$8	$8	$4	**$40.5**



Crisis Evaluation and Management Technology Roadmap

Chapter XI

All-Source Situational Understanding (ASU)

Chapter Chair: Hal Kempfer
Chapter Coordinator: Michelle Royal

Definition

All-Source Situational Understanding (ASU) is the ability to perform four interrelated tasks in order to have the earliest possible, specific, and continuing knowledge of a threat, and to support incident command decisions across all phases of a local or regional response:

- Collect and identify threat-relevant information;
- Fuse and analyze information to support threat awareness;
- Identify persons who need to know specific types of information (and what that information is); and
- Disseminate appropriate information to (and only to) appropriate persons.

As a threat crosses jurisdictional and even state lines, so must information. A crucial element of this ability is the need to make information readily available and useful to all relevant actors across disciplinary, jurisdictional, and geographic lines, as appropriate to a particular evolving event, without compromising the security of this information. Skillful use of ASU speeds response by decreasing response time, decision time and time required for course of action (COA) development.

Operational Environments

The operational environments most relevant to all-source situational understanding are derived from the operational progression of an event, representing phases of the "intelligence process" in supporting incident command before, during and after a threat manifests itself, as well during consequence management and restoration. The Operational Environments are defined as:

- Awareness
- Alert and Warning
- Crisis Response and Threat Reduction
- Consequence Management and Restoration

Needed Functional Capabilities and Priorities

The needed functional capabilities prioritized in the Emergency Responders' workshops include the following items, prioritized in order of importance to the responders.

- Threat Assessment/Data Collection/Analysis
- Intelligence Preparation for Operations
- Threat Relevant Data Distribution
- Intelligence Support to Unified Incident Command Structure

Overall State of Technology for All-Source Situational Understanding

While responders believe that they have marginal capability for each of the functional capabilities, the technologists rated the technologies to enable these capabilities as available in the near-term, if not currently. *Threat Assessment/Data Collection/Analysis* (ASU.1) and *Intelligence Preparation for Operations* (ASU.2) are the only capabilities which should require technology development with a moderate degree of risk. All

All-Source Situational Understanding

Functional Capabilities	Operational Environments: Preparation and Awareness	Alert and Warning	Crisis Response and Threat Reduction	Consequence Management and Restoration
1. Threat Assessment/Data Collection/Analysis				
2. Intelligence Preparation for Operations				
3. Threat Relevant Data Distribution				
4. Intelligence Support to Unified Incident Command Structure				

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

- The ability to integrate information among several different jurisdictions and levels of government.
- The establishment of processes that allow quick data validation, using information on data source.
- The ability to link information/analysis and detection across different sources.

other technology areas can achieve results with low technology development risk.

ASU.1 – Threat Assessment/Data Collection/Analysis. *The ability to collect and identify/recognize threat-relevant information (i.e., indications and warning), validate and analyze the data, and validate and assess the threat for purposes of evaluating threat levels and credibility.* Note: this functional capability is crucial to the overall value of the ASU NTRO.

Goals:

The goals identified by responders for this area include:

- Ability to provide all relevant jurisdictions and disciplines access to near-real-time, same-quality information and an awareness of the threat. Responders defined near real-time as being within 15 minutes. They saw this as the time when the information product has "real value."
- Ability to collect, validate and fuse information from several disciplines (technical as well as observations from patrol officers, firefighters, epidemiologists, and other responders), especially automated open-source information.
- Threat assessment toolkit that aids in pattern recognition and validating data.
- The establishment of processes and systems that foster redundant analysis and competition among analytical hypotheses.
- The ability to analyze multi-disciplinary (*i.e.,* not just law enforcement-originated) threat assessments.
- The ability to centralize pooling and synthesis of distributed or multiple sources of analysis, with access to all sources of threat information and updates, including electronic clearinghouses (*e.g.,* FBI's Law Enforcement Online and RISS-ATIX).
- The ability to support unconstrained "thinking outside the box" rather than forcing analysts to consider limited or non-creative hypotheses, options, etc. (no blinders on analysts). This is "red teaming" at its most useful.
- The ability to integrate tools for data mining of both structured and unstructured information, geared toward detection of changing trends (*i.e.,* early detection of emerging threats), detection of alert situations including anomalous detection via normalization, automated foreign language translation including understanding of context supported by cultural intelligence, and processing of images, video, audio and signal data with automated extraction of text and image data elements.

Current Capabilities:

There are indications and warning (I&W) processes currently used by responders, but rarely are they formal or disseminated as in the military. The military uses I&W in a combined human, analytical and information technology-assisted process that quickly identifies patterns and trends which enable the development of broad intelligence collections plans (*i.e.,* sensors) to "watch" named areas of interest (NAI). For example, in an urban environment, if an underground passageway is a likely avenue of approach for intruders to a particular building, then movement of personnel though that passageway could provide (tactical) I&W of a possible rehearsal, probing, infiltration or attack. Unattended ground sensors or motion detectors could be used on this passageway, and the passageway would probably be designated an NAI. Responders face similar issues; however, tactical I&W generates a very small window in which to make that intelligence actionable. It is difficult for responders to analyze this information while responding to an event, disaster or incident using the current, well-accepted and well-proven concepts of operation in public safety. Integration of I&W as a capability requires modification of current operating procedures.

Responders noted that, currently, a fire captain or fire chief is likely to be the Incident Commander, but this fire chief is not normally inside the information "loop," at least not to the same degree as law enforcement. There is a need for fire officials, and other non-enforcement officials, to get federal security clearances granting them access to current threat intelligence. As intelligence information comes in, especially that dealing with potential WMD threats, responders need to intervene by taking preventive or mitigating steps early on. Since fire officials normally don't have clearances, they won't get the information early when they can do the most with it.

Another alternative is to maintain an open source information analysis capability, which does not currently exist. The lack of familiarity in dealing with intelligence information risks operational compromise of that information. For smaller jurisdictions, the needed information technology is simply not available. If given the technology without proper preparation and planning, it will be poorly utilized. If the government intends to provide these smaller jurisdictions with technology, it will need to assist them with:

- Need assessments (*i.e.,* what do we really need?)
- Training on how to use it
- Integration of technology into current operations

Responders noted that the critical need is for "tailored" intelligence, not just data dumping. Not everyone needs to know everything, but those who do need to know should be getting it. For example, if the fire department is responding to an address and there is threat information that says this could be a highly dangerous situation, then that "intelligence" needs to get to the initial responders (prior to arriving on scene) for course of action development.

Responders specifically noted some of the crisis management software packages that provide collaborative and situational awareness tools, and interoperability with other tools. Their browser-based software links the key players in a response for multi-agency, multi-jurisdiction collaboration, and for sharing a common operational picture and information. One of the tools includes:

- Incident Reporting and Tracking
- Critical Infrastructure Reporting
- Situation Reporting
- Action Planning
- Personnel Management
- Alert Notification
- Real Time Messaging

Los Angeles area law enforcement uses the War Room of the Los Angeles Clearinghouse. An

enforcement operation is plotted on an electronic Thomas Brothers map, where it is automatically geo-assessed with regard to any other events occurring in the immediate vicinity. If there is other law enforcement activity, especially undercover operations, an audible and visual alert will activate. War Room personnel would then notify both active groups of their respective operations. There have been cases where undercover groups unbeknownst to each other are actually conducting enforcement operations on the same location, resulting in a "blue-on-blue" confrontation. This automated GIS technology has prevented this from happening on several occasions, probably saving the lives of officers and special agents.

State of the Art:

The enabling technologies for this functional element include geospatial visualization and mapping technology, automated link analysis systems, database access and mining techniques, collaboration technologies and non-structured information analysis and visualization technologies, all brought together with integrated command, control and communications systems (C^3I). There are multiple COTS technologies in this area; unfortunately few of them operate on a single platform.

In terms of mapping software, there are only a few main vendors who provide the sort of integrated graphic software package that can allow graphically depicting "map data" as broader intelligence products. Specifically, this involves using this sort of GIS product for uncovering hidden connections or inconsistancies requiring further investigation. Some of these are:

- Early into the Bosnia mission, one commercial provider adapted its GIS ArcView package to include embedding critical data fields and imagery onto electronic maps that allowed commanders and their staffs to "drill down" on specific locations, especially in urban terrain. The latest intelligence could be graphically embedded, providing the commander an ability to visualize the battlespace and pull up important information about that area to shape his decision-making.
- Technologists in the workshop mentioned industry innovations which extend the performance of these systems by providing peer-to-peer collaboration, distribution, visualization and analysis of GIS data layers. These systems utilize standard Web browsers and Microsoft Office documents to collaborate with geospatial information. Interaction is in 2-D, 3-D or 4-D and is extended for use with standard email, chat rooms and instant messaging.
- There is at least one COTS product that breaks down data into the simplest form and then maps it to find common links. Thousands of items are analyzed simultaneously for cross-referencing. The deliverable product is a very different kind of "map" that shows links between persons, places or things. Other COTS software offer link and network analysis, timeline and transaction analysis. Many of these systems automatically link to GIS to array information geospatially. Just after September 11th, these products suddenly saw a rise in demand from military users working counterterrorism research and analysis. Some of these companies have moved into the competitive or business intelligence market with link analysis software for use in the commercial world, which has potential application to analyze criminal enterprises like terrorist networks or drug cartels.
- With regard to access databases and data mining, there are many companies who sell large open source data bases such as the public record databases most commonly used by insurance investigators. LexisNexis™ provides substantial legal, news, public records and business information; including tax and regulatory publications in online, print or CD-ROM formats. These can be viewed using various types of proprietary products or services by occupation, industry or task. LexisNexis has application software that can integrate technologies and content to support critical decisions-making as well. In addition, there are companies that sell databases that provide past employment records, education

verification, criminal history, and other background information. More than 5000 companies use one such service which is widely used for employment screening information.

- Open source databases, even proprietary ones like those described above provide investigators with the ability to find information on persons, property, businesses, trends or other elements of interest that may not appear in criminal databases, or be fully available through other official government databases. For the most part, these information firms buy public records, or information from private sources such as the media, professional publications, etc., and then put them together in large databases that are enabled with software search processes.

- The Defense Information Systems Agency's (DISA) Area Security Operations Command and Control (ASOCC) is an ACTD that was developed after September 11th. ASOCC combines advanced information-handling tools with command and control tools for homeland security purposes, linking all of the communications capabilities with the National Military Intelligence Center (NMIC) and the military command authorities, as well as to the regional intelligence centers and civilian authorities, including law enforcement agencies. Civilian law enforcement entities included within the ASOCC ACTD include the Federal Bureau of Investigation, U.S. Customs and Border Patrol (CBP), the Drug Enforcement Agency, U.S. Immigration and Customs Enforcement, and the Coast Guard, along with their associated intelligence entities. After September 11th, DoD quickly realized that no such "linkage" capability existed; so ASOCC was developed.

- Another program specifically referenced by responders and technologists is the Capitol Wireless Integrated Network (CapWIN). CapWIN provides a "communication bridge" allowing mobile access to multiple criminal justice, transportation, and hazardous material data sources. In essence, it is a state-of-the-art wireless integrated mobile data communications network being implemented to support federal, state, and local law enforcement, fire and emergency medical services (EMS), transportation, and other public safety agencies primarily in the Washington, DC Metropolitan area. The purpose of CapWIN is to greatly enhance communication and messaging systems, effectively creating the first multi-state, inter-jurisdictional transportation and public safety integrated wireless network in the United States.

- The federally sponsored Disaster Management Integration Services, or DMI-Services provides a capability for the consequence management community to share digital information. DMI-Services provides a series of basic automated tools. These tools are designed to give organizations the "starter set" of applications that will enable them to share digital information with others agencies.

- Workshop participants referenced Cybercop. The Cybercop Secure Portal was developed as a volunteer private sector initiative as a result of Presidential Decision Directive 63. The Cybercop Secure Portal has its roots in a secure computer mediated communications project created at DARPA (Extranet for Security Professionals or ESP). It uses 128 bit SSL encryption technology to create an online gated community where law enforcement and information security professionals can securely communicate and collaborate. The portal links over 1,400 users and contains over 700 files in its libraries with a focus on homeland defense, critical infrastructure protection and cybersecurity issues. Currently, Cybercop is highly integrated with FBI's InfraGuard program.

Also important to this function are technologies that support the analysis of non-structured information and data fusion for all-source situational understanding. Starlight is an advanced three-dimensional visualization technology that was developed by Pacific Northwest National Laboratory (PNNL). It helps solve the problem of information overload. It has been used by the

U.S. intelligence community, but can be applied to a variety of other fields, such as medical data analysis, environmental security and current events monitoring. Starlight uses a tool for non-structured information software called GENOA. GENOA is a customizable, front-end retargetable source code analysis framework. Starlight is a visualization tool that will be integrated into the GENOA system as part of the development of new and complementary visualization tools. A collaborative investigation of the use of Starlight in the Southern California area shows that the tool has operational utility but needs modification for local public safety use. Local and regional public safety operations will require a networked operational capability which is not currently inherent in such operations. Starlight, or a similar tool, could be of great value in developing such a regional operational capability.

There are no national standards or cooperative operational procedures in this area. Various national bodies such as the IAB (Inter-Agency Board), LEWG (Law Enforcement Working Group) and OLES (Office of Law Enforcement Standards) have sub-groups trying to establish standards.

Technology Limitations and Barriers:

As the foregoing discussions indicate, technologies to support the goals in this functional area exist and are commercially available. Integration of these technologies, many of which are proprietary, would facilitate the needed capability. Some of the most vexing technical limitations involve the same challenges found across the entire command, control, communications and information management spectrum: integration with legacy systems and communications capacity (bandwidth). These challenges are being aggressively pursued across the industry.

The barriers to attaining these goals are intelligence community administrative and policy issues, cultural differences between responder and national security communities, the lack of national standards, and most significantly, the lack of funding support at the local level. In our workshops, responders and technologists pointed out that we are a "crisis-oriented society." Issues related to all-source situational understanding are often long-term and low profile. Since the squeaky wheel gets the grease, money for law enforcement typically gets siphoned off into easily explainable items such as putting more sworn police on the streets or buying new cars or other enforcement oriented equipment.

Gap Fillers:

A nation-wide trusted collaborative infrastructure that can be used to share sensitive information is a requirement. A national response All Source Situational Awareness prototype system, which combines the integration of the latest technology with the development of new concepts of operation that support incident command with intelligence analysis and information sharing, would be a useful step in filling this capability gap. The prototype system and process could be emulated by and coordinated across local regions. The goal of affordable implementation should be a program objective. The system must include the high-bandwidth communications necessary.

ASU.2 – Intelligence Preparation for Operations (IPO).

The ability to: (1) identify which agency, office or official is responsible for collecting and analyzing which types of intelligence, and (2) implement tools, training and processes to support those responsibilities.

Goals:

- Automated systems for information sharing and notification of intelligence responsibilities
- Minimal redundancy in intelligence dissemination
- Maximum access to needed information and background for those who need to know and have the responsibilities
- Information and facilities technologies to support different levels of clearance and classification, for seamless sharing of information among those with responsibilities, irrespective of different clearances and venues.

- Information sent via our channels and appliances that are not open to unauthorized users or the public.
- Regional clearinghouse for data analysis to support nearby smaller jurisdiction without the manpower for an all-source situational understanding capabilities.

Current Capabilities:

The concept of "Intelligence Preparation for Operations" (IPO) originally stems from the military doctrine called Intelligence Preparation of the Battlefield (IPB). It is a rigorous process of looking at a particular area of terrain wherein friendly forces are anticipating or planning operations. IPB centers on three principal features: weather, enemy and terrain (WET). During the deployment of the Combined Joint Task Force – Consequence Management in the Persian Gulf in 2002, this acronym was modified for civil-military purposes to WETT, or weather, enemy, threats and terrain. Part of this WETT modification was directly related to the emerging civil-military concept of IPO.

By definition, IPB is a continuous process defined as:

- Define the battlefield environment
- Describe the battlefield's effects
- Evaluate the threat
- Determine threat COAs (Courses of Action)

Responders however, are not on a "battlefield," but instead conducting operations in their locales. However, if the "battlefield" is changed to "operating area," it also changes the context and substantive meaning for responders. For example with this simple change the four processes become:

- Define the operating area environment
- Describe the operating area's effects
- Evaluate the threat
- Determine threat COAs (Courses of Action)

If "threat" is broadened to mean anything that can threaten lives or have an adverse impact on operations, it changes the traditional concept of IPB from being focused on the enemy, to being focused on preparing responders to plan and conduct a broad array of emergency operations. In assessing the urban environment, information must be collected on a number of "friendly" factors and assessed with the same process as one might assess the "threat." This could include information on businesses, and municipal government and other entities that could assist or hinder operations. Demographic and socio-political factors must be understood also. There are ample examples in the US and overseas where emergency operations have been hindered by public mistrust of response forces, gross misunderstandings of what is being done, or enemy information operations meant to seed both distrust and confusion.

IPO as a doctrinal term was developed by the Los Angeles Terrorism Early Warning Group (LA TEW). It has several components that take the traditional intelligence cycle, and then "spoke" out in various directions to develop a comprehensive fusion process. The term "intelligence" is often misunderstood. Doctrinally, intelligence is an analyzed information product. Collected raw data is synthesized and fused into useful information. While that information could be acted on as presented (and frequently is), the information is further analyzed to draw out more inferences or conclusions, which becomes an "analytical product."

The Los Angeles Terrorism Early Warning Group develops and maintains a series of target folders (description of possible terrorist targets) and playbooks in preparation for a large variety of potential threat scenarios and venues. It uses an all-source, all-discipline, all governmental level approach in evaluation intelligence, and a network methodology for sharing and disseminating sensitive information. Unlike other "intelligence fusion centers," such as the FBI Joint Terrorism Task Force or California Anti-Terrorism Information Center, the TEW concept includes responders and analysts representing federal, state, local, military, national agencies and critical

industries. That way, the LA TEW ensures its input processes, collection methodologies and products meet the larger crisis and consequence management needs of fire, health, enforcement and the greater intelligence community. Although there are other systems that have better equipment and software, as well as better connectivity to national systems, those tend to be limited to the law enforcement community. The LA TEW is working on improving these issues.

The Pierce County, Washington TEW has taken the next step by automating a number of key files. A particularly apt example of this automated IPO product's potential occurred in Spokane, Washington, at Lewis and Clark High School. The school had plans of the school available on-line through a secure system called Rapid Responder. This system provided responders blueprints, photographs, evacuations plans and lists of hazardous materials. The plans also showed such key features as windows and doors. locations of security systems, shutoffs for utilities, and a photographic layout offering a 360 panoramic view that includes rooftops, gymnasiums, libraries, auditoriums and other gathering places. The database includes phone numbers and all emergency plans. In late September 2003, a disturbed 16 year-old came to school armed, and took over a classroom telling the teacher and students to leave. SWAT members were able to readily access the Rapid Responder database, discover a second door to the room, and conduct a timely and successful take down of the perpetrator, thereby proving the value of this type of automated "intelligence preparation for operations" product for responders.

Originally, the DMI-Services, was placing what were essentially target folders and playbooks, along with other kinds of venue plans, imagery and related response information online. However, online information security is a big concern with regard to dissemination of IPO related information. A recent example of how bureaucracy can sometimes run astray of intent occurred when the Los Angeles Metropolitan Water District requested a vulnerability and hazard assessment of its system due to homeland security concerns. As part of the bid process, they posted detailed plans of the water system online for potential vendors to review. This "vulnerability" was eventually brought to their attention and taken off the Internet, but not before the information was accessed (and presumably downloaded) by overseas email addresses in Pakistan and elsewhere in South Asia.

Threat assessments from some of the criminal intelligence clearinghouses are probably the closest products to anything resembling IPO. On the drug enforcement side, the "Threat Assessment" actually comes from a related "center" (the Joint Drug Intelligence Group) run by the FBI. That product is mostly distilled statistics on enforcement actions geared towards justifying funding of regional counterdrug activities. Threat assessments on the terrorism side have focused on critical infrastructure and been principally done by National Guardsmen trying to apply IPB doctrine. This has resulted in lengthy lists of potential targets covering the state. In Minnesota, the National Guard has developed a separate methodology for this kind of critical infrastructure assessment process, and a quantitative model used to assess the vulnerability or criticality that various utility, industry or other "infrastructure" represents.

One example of information sharing and collaboration that the workshop participants identified was the Statewide Anti-Terrorism Unified Response Network (SATURN) program in Massachusetts. SATURN is an information sharing and responder network that builds on current systems. It provides fire and emergency management personnel a process for exchanging information, and for providing training and coordination of anti-terrorism strategies tied to collaborative public safety capabilities. SATURN is a Web-based information sharing architecture that brings together federal, state and local first responders and emergency management with designated citizen groups called Citizen Mobilization Teams (CMT).

Responders also identified the Consequences Assessment Tool Set (CATS). CATS is a joint

ESRI and SAIC program that provides a comprehensive package of emergency management decision aids, including hazard prediction models (natural hazards and technological hazards) and casualty and damage assessment tools. It also accepts real time data from local meteorological stations. The tool set is supplied with over 150 data bases and map layers. These include the location of resources to support response to specific hazards, infrastructure objects and facilities (communications, electric power, oil and gas, emergency services, government, transportation, water supply), a variety of population breakouts and much more. It also allows the user to add databases for custom analysis. However, like nearly all hazard prediction or plume modeling software, it is unable to do detailed modeling for complex areas in urban terrain, but rather uses a model of open terrain, like a traditional battlefield.

Fire pre-plans are an "intelligence product" widely used by emergency responders. These are normally hard copy documents that include layout and fire-specific criteria of buildings that can be used in an emergency. These are rarely automated, and fire services normally have neither the necessary digital communications nor the information technology available to support such automation. Currently, most large buildings and facilities submit plans to the fire department. Regulations require blueprints for tall building to be on hand in the lobby for responders to reference as needed in cases of emergency. All of this data could be digitally archived for immediate retrieval, and for data manipulation (*i.e.,* 3-D projection) using various advanced software applications. The ability for emergency responders to "see" into buildings using this type of data is generally available now. Fire inspectors routinely visit buildings and are able to update files, and image the inside of various buildings. Urban wargaming techniques currently being evaluated by some agencies may offer the ability to assess the tactical threat of urban buildings in a fashion similar to a military assessment.

State of the Art:

Several companies have teamed up on a concept called Active Citizen, with the goal of creating a community communication architecture to connect citizens, augment responders and provide critical cultural information for public safety and law enforcement. Active Citizen has three steps within what is termed a Community Intelligence Coordination Center (CICC) that begins with:

- *Data* – All source reporting.
- *Information* – What is happening.
- *Knowledge* – Context.

The end-state of CICC is to enable decision support with products such as planning tools and environmental, cultural and incident scene information. All of this is fed to public safety and law enforcement agencies. It is a community-based approach that empowers citizens as partners with law enforcement in the effort to protect their neighborhoods and communities, with the idea that an alert and trained public is the greatest deterrent to attack. At the center of the model is the cyber citizen corps portal that feeds in environmental data, cultural data, specific information requirements, incident situation reporting and even damage assessments. The CICC's products are cultural analyses, environmental risk mitigation, pattern recognition and GIS products. It is anticipated that this capability could grow to include video teleconferencing (VTC) and a virtual emergency operations center (EOC). In its final form, the cyber citizen portal would be the collaborative center linking the federal information center, state information center, local law enforcement and community.

Tied in with Active Citizen is the Domestic Emergency Response Information Service (DERIS) concept. DERIS demonstrated the feasibility of a portal approach to law enforcement crisis response. It implements National Institute for Urban Search and Rescue standards for extreme information infrastructure, and can

act as a prototype for civil military C2 (command and control) supporting the Common Operational Picture (COP). DERIS was tested using the Burning Man annual event in Nevada and then at Shadow Bowl, an exercise that simulated a Super Bowl in San Diego with a relative degree of success.

Active Citizen and DERIS provide a number of information tools, such as:

- *Prepared Response* – an automated target folder archive.
- *CyberCop* – ESP's free secure collaboration portal.
- *Netowl* – a knowledge mining tool.
- *Virtual Operations Center* – MindTel's modified version of a virtual 3-D workspace tailored for emergency management and law enforcement situational awareness.

Technology Limitations and Barriers:

The barriers to accomplishing IPO are not primarily technical. As in any information technology enabled function, there are concerns about available bandwidth and whether the communication and information management infrastructure can support the multilevel security needs of processing intelligence. These problems are being addressed in other areas. We simply have little experience in moving information, especially intelligence information, around the responder community during a major incident. Until September 11th, there was little motivation on the part the federal government to establish strong intelligence sharing relationships with the responder community, especially outside tight law enforcement circles. Before September 11th, very few people considered the response to an incident as "battlefield" for which intelligence needs to be prepared. Funding priorities, training requirements and cultural adaptations have yet to catch up with the need.

Gap Fillers:

Some of the concerns with IPO stem from information sharing, and the quality of intelligence analysis. A highlighted concern voiced by workshop participants is the need for a regional clearinghouse for data and analysis to support nearby smaller jurisdictions. NYPD has a substantial clearinghouse capability, but this is mostly supporting operations within its own jurisdiction.

As previously mentioned, the Los Angeles Country Regional Criminal Information Center (LACRCIC) or the "the LA Clearinghouse" performs this function. It is a combined center that has a 24/7 data sharing/research and event deconfliction center, along with analyst groups that provide case support. It is also home to the California Anti-Terrorism Information Center (CTIC), which leverages its capabilities from the same infrastructure.

In California currently, the "clearinghouse" focuses almost solely on criminal intelligence, and is tied in with the Los Angeles High Intensity Drug Trafficking Area. Their methodology is placing "analysts" in support of criminal investigations, whether it is against drug traffickers or terrorists. There is a need to develop and deploy a benchmark IPO process for responding to a terrorist threat. The federal government should develop such a process which can be used by regional authorities as a template for creating a similar indigenous process.

ASU.3 – Threat-Relevant Data Dissemination.

The ability to (1) identify what kinds of threat-related information must be disseminated, (2) identify who must receive what information (i.e., need-to-know), and (3) deliver the appropriate information among disciplines only to the appropriate agency, office, or official.

Goals:

- Integrated secure system of delivery
- Identification of need-to-know criteria.

- Methodology for transmission of timely, in-real-time knowledge and confirmation of such receipt.
- Smart and timely 24×7 intelligence dissemination (emphasis on timely receipt).
- "Smart Security" in dissemination technology and methods, according to kind of information. Level of security (and hence dissemination method, *e.g.,* fax) depends on the kind of information: open channels sometimes appropriate.
- Dissemination, security and access issues taken into account at the regional operational level, not hoarded at the individual department or functional agency level.

Any dissemination system must also maintain assured operational security (OPSEC).

Current Capabilities:

The consensus among responders is that there is only marginal capability to disseminate threat relevant data to the responder community. An example of this is the information that does or doesn't accompany the Department of Homeland Security's National Terrorism Alerts. Among the concerns were that there is no intelligence capability to adequately disseminate sufficient information to compliment what is essentially an operational threat condition change, and that this system is not tied to a nationwide IPO process for moving intelligence information or assessments either to or from the local, state and federal levels.

This problem is partially characterized in the debates over PUSH vs. PULL intelligence. With email dissemination, there is a problem with getting the "spigot turned on" by being part of various Homeland Security or Terrorism Threat information groups, both open source and closed. Traditional "push" intelligence under the current system creates information overload, with the same effect as too little information, producing the equivalent of spam emails on terrorism or related threats. This push methodology overwhelms the recipients. This effectively turns the police chief or fire chief into a de facto intelligence analyst, since there are no effective filters or additional assessment processes to tailor the information for specific needs or requirements. Pull dissemination, in contrast, requires an active search to find needed information. Much of the information pull capability today is Internet-based. A simple example would be a Google search.

The debate is ongoing in the military with the proliferation of information on the battlefield. The 1st Marine Expeditionary Force moved to a pull-based information environment focused on Web-centric dissemination of critical information. Even before September 11th, 1st MEF staff and commanders were overloaded with emails on the host of operations, plans and administrative information dealing with contingencies covering two-thirds of the globe. For the most senior personnel, this meant they would get hundreds of emails daily using the traditional push method of dissemination. As one senior staff officer at 1st MEF put it, "the Commander has become the senior analyst," hence the change in the method of information access.

Emergency responders note that systems using a pull method for homeland security or terrorism information, such as a Web-centric system, should include secure access, information posting, a tailored alert system using specific parameters and a drill up/drill down capability to support analysis, as it is needed. Supporting technology probably exists, but is not obvious or easily available to public safety emergency response organizations.

Both the issue of information classification and the handling of classified information are significant elements in information sharing that must be addressed. The Department of Defense (DoD), as noted in Crisis Evaluation and Management, has initiated several projects to address the capability to exchange information and data through an automated multilevel security system (MLS). These issues are significant for public safety first response.

Among the many law enforcement telecommunication systems in the country, the Oklahoma Law Enforcement Telecommunications System (OLETS) appears to be a benchmark. It is a private, leased-line, digital telecommunications network maintained by the Oklahoma Department of Public Safety. It serves over 750 police departments, county sheriff's offices, highway patrol headquarters, military bases, and emergency operations centers (EOC), and other agencies concerned with pubic safety and law enforcement. OLETS agencies communicate through a central message switching computer housed at OLETS headquarters in Oklahoma City that allows those agencies to query central databases in search of criminal records, license and registration information. OLETS also allows them to communicate with other agencies across the state and nation, and access information tables that reside at the OLETS switch.

InfraGuard, an FBI-industry collaboration focused on the cyber-security and the information technology sector may be a good benchmark for two-way communication of threat information. The national InfraGuard program began as a pilot project in 1996, when the Cleveland FBI Field Office asked local computer professionals to assist the FBI in determining how to better protect critical information systems in both the public and private sectors. Today it is a joint teaming project linking the private sector with the U.S. government, or more specifically the FBI. The initiative was developed to encourage the exchange of information by the government and the private sector members, and private sector members and an FBI field representative form local area chapters. With hundreds of company members across the nation, there are now 79 active chapters of InfraGuard. The Federal Bureau of Investigation acts as the facilitator by:

- Gathering information and distributing it to members;
- Educating the public and members on infrastructure protection;
- Disseminating information through the InfraGuard network;
- Producing analytical products on information received through the InfraGuard network;
- Expanding communication between government and private sector members.

State of the Art:

Responders and technologists pointed to the Tulsa Area Syndromic Surveillance System (TASSS) program as a benchmark in biological or epidemiological intelligence (*i.e.,* epi-intel) sharing and dissemination. It looks at all key data fields and ties into the labs, especially for trend identification. TASSS's objective is to alert medical professionals to the possibility of significant outbreaks before large numbers of patients present with advanced stages of disease. It is a partnership with area hospitals by electronic transfer of emergency room chief complaints into the TASSS model with analytical focus on five principal syndromes: fever, rash, respiratory, diarrhea, and vomiting. TASSS, which is maintained by the Planning and Epidemiology Division of the Tulsa City/County Health Department, can be accessed through the Internet with proper clearance, and is a key component of the new Tulsa Terrorism Early Warning Group program. Other sites that are being considered to expand the epidemiological surveillance program of TASSS include schools, clinics and major employers.

The needs of responders to conduct IPO are not unlike those of power grid management and there is technology in that industry that could be adapted for emergency response. The Department of Energy's Pacific Northwest National Laboratory (PNNL) has been working on this power grid reliability, from the impact of aging infrastructure, deregulation, and the vulnerabilities to terrorism. PNNL envisions a power grid of the future through its Energy Systems Transformation Initiative. Called GridWise™, it enables collaboration among generators, the grid and customer loads to collectively increase the stability and cost-effectiveness of the power system. It applies solutions for adapting and influencing information, and control technology approaches to deliver reliable energy.

GridWise is a regionally networked, but also decentralized approach, using smart chips that would be fitted onto household appliances and would continually monitor fluctuations in the power grid. In high periods of stress for the grid, a "grid-friendly" appliance would identify fluctuations and automatically shut down. Brief interruptions of 5 or 10 minutes of time give the grid operators time to stabilize the system, but wouldn't be noticeable to the consumer. The idea was that it would potentially stop a cascade effect similar to what happened in the Northeast when the whole grid essentially collapsed. Smart appliances could also stagger return to service after an outage and thus ease the restoration of power. From an IPO technology standpoint, it is a decentralized information collection and assessment process that facilitates a flexible response to an emergency situation.

Another benchmark medical surveillance system is the Emergency Medical Alert Network (EMAN) of San Diego County. EMAN was developed by the Epidemiology Division of the San Diego County Health and Human Services Agency (HHSA) in December 1999. EMAN is intended to expedite confidential communication between healthcare and public health professionals in San Diego County. Fundamentally, it is a network dedicated to facilitating bi-directional confidential communication between San Diego County's medical community and public health and safety agencies in order to ensure rapid identification of and response to unusual disease events or public health emergencies.

Another example of collaborative communication of security information is the Overseas Security Advisory Council (OSAC). Through OSAC, U.S. companies, to include public and private colleges and universities, are provided timely information in which to make informed corporate decisions on how best to protect their investment, facilities, personnel and intellectual property abroad. It was established in 1985 by the U.S. Department of State to foster the exchanges of security-related information between the U.S. Government and American private sector interests operating abroad. OSAC is currently administered by the Bureau of Diplomatic Security, and has developed into a productive joint venture for effective security cooperation.

One example of an emerging enabling technology is Situation Management and Awareness in Real Time (SMART), a tactical command and control system developed by International Aerospace which enables the secure, two-way exchange of information and intelligence over a low-bandwidth, public network. The software is designed to correlate, integrate and update data, information and intelligence from a wide range of sources. It supports display of its Common Operating Picture (COP) or Single Integrated Picture (SIP) in near-real time and in interactive 2-D and 3-D formats. SMART uses a "one-to-many" peer to peer network, and is intended for use in tactical operations involving networked tablet computers or PDA's. Described as 'glueware,' because it links incompatible command and control or information systems, each SMART unit has the ability to connect to a GPS receiver or a vehicle interface and could be used to disseminate its position and all associated data with that unit.

Technology Limitations and Barriers:

The most significant barrier to dissemination of threat-relevant data may be the restrictions on classified data. The technical and administrative infrastructure required to store and disseminate classified material is not available in the responder community. To implement such a system would require granting clearances for thousands of additional people and the implementation of additional secure networks over which to transmit the data. Significantly increasing the dissemination of data to the responder community will require a large and expensive effort and it will be primarily the responsibility of the federal government.

The implementation of technology to assist incident commanders requires significant investment in time and effort to achieve, but minimal investment to develop. Most of the useful or applicable technology is either available or will be in the near term. A significant challenge will be to scale

the national dissemination system to effectively support the responder community while safeguarding sensitive information.

Gap Fillers:

The technological building blocks for developing a threat dissemination system appear to be present in many of the products sited above. Some tailoring of those will be necessary. The capability gap seems to be the ability to integrate information processing systems. This issue could be resolved by developing a national standard to which regional authorities can build.

ASU.4 – Intelligence Support to Unified Incident Command Structure.

The ability to provide valid intelligence assessments (including estimates of threat capability, intentions/targets and trends/potentials), damage assessments/reports, resource capability and availability, recommendations for courses of action, and timely situation briefings, in an operationally useful and real-time process, to the incident commander/unified command at all phases of response.

Goals:

- Support real-time decision making.
- Seamless integration with other related Functional Capabilities.
- Enable maximum use of visual methods to display needed information.
- Insulate incident command intelligence briefings and decision-making from chaos and distractions.
- Incorporate reports from the field (down-range) real-time into the intelligence product as updates for the overall situational understanding.
- Allow the incident commander to disseminate decisions with relevant intelligence "attached" to the command.
- Enable "rolling" documentation of lessons learned as the crisis evolves.

Current Capabilities:

Many of the functional needs in this area are the same as those required in ASU.1 (*Threat Assessment/Data Collection/Analysis*), ASU.2 (*Intelligence Preparation for Operations*) and ASU.3 (*Threat Relevant Data Distribution*). Therefore, only the differences will be addressed here. As was the case in the preceding functional areas, the responders and technologists who participated in Project Responder felt that this capability was marginal today. One problem noted at the national level is that the capability is very difficult to develop and maintain if local officials choose not to use the Incident Command System (ICS) and its structure. Use of the ICS is considered the essential building block on which to build a doctrinal intelligence fusion capability. Currently, use of the ICS is not universal. Political acceptance and establishment of a national model for both developing and feeding intelligence to an incident commander is required to set up and implement processes like the one described here. The use of the ICS nation-wide is considered essential.

In order to provide intelligence support to unified command we may look to the military for examples of current capability. At the UIC level, there is a need for an all-source intelligence fusion center (or IFC), similar to a military Joint Intelligence Center (JIC) or Joint Intelligence Support Element (JISE). The size of these intelligence fusion elements is scalable. For example, a JIC may have hundreds of personnel. By contrast, a JISE is normally for a smaller joint task force with a headquarters of 100-300, and is normally has a dozen or dozens of personnel assigned.

Typically, a military IFC (JIC/JISE/IOC) will have a surveillance and reconnaissance center (SARC) either embedded or adjacent for immediate feed from all sensors or reconnaissance assets; ground, air, maritime, human or mechanical. They will become the center of data feeds for all IMINT/imagery, HUMINT/human, SIGINT/signals, ELINT/electronic, MASINT/measurement and signature, and any other form of collections assets that provide raw intelligence. In a

typical enforcement operation, collecting information from witnesses or informants would fall under HUMINT. The IFC may also have plans, operations and fusion or analysis sections that support all of these functions, along with those technologies needed to develop and maintain the common operational picture or COP, or that portion of it that is sometimes called the common intelligence picture or CIP.

The intelligence directorate or section using it is involved with all facets of the intelligence cycle process that includes: Direction and Planning, Collections, Fusion and Synthesis, Analysis and Production, Dissemination, Utilization, and the inputs back to Direction and Planning. Normally, the intelligence fusion is often focused on what is called intelligence production, or turning out finished products for operational consumption or utilization. Within non-traditional military mission spectrums, there is the potential for functions involved with collections planning and management that may fall under the intelligence fusion center, and since that requires a high degree of operational assets that have dual capabilities for collection information and data (*i.e.,* responders, investigators, aircraft, etc.), this role must be clearly defined early on with senior executive intent stated and widely understood. Having an IFC, enabled by the latest technology and reporting directly to the unified or incident commander is the key to this functional capability.

State of the Art:

The Incident Command Information Tool (ICIT) is an example of current technology that can address this issue. The incident commander needs real-time video capability on-site. As proven during the Democratic Convention in 2000, monitoring the media is critical to supporting decision-making by the incident commander, since so much of what is being done and communicated has far-reaching consequences and the IC must be responsive to the elected leadership.

As mentioned previously, the federally-sponsored Disaster Management Integration Services, or DMI-Services provides a capability for the consequence management community to share digital information. This stemmed from key development work with the Consequence Management Information System (CMIS) working with the Marine Corps Systems Command prior to September 11th. DMI-Services has expanded upon this to provide digital information solutions in an all-hazards disaster incident command response environment.

Defense Advanced Research Projects Agency's (DARPA) Command Post of the Future (CPOF) has a number of relevant technologies. CPOF includes a Command Post Information Environment (CPIE) that will provide new ways to collaborate and to interact with supporting information assets and sources. Included in this, the Navy is developing both 2-D and 3-D virtual reality (VR) tools that enable better battlespace visualization by commanders in the CPOF. CPOF components include:

- Access to information and control devices via PDAs.
- Speech recognition from microphones throughout the center.
- Interactive 3-D visualization.
- Gesture recognition.
- Tailorable information awareness.

A number of these technologies would be very helpful in getting intelligence and situational awareness information directly to the incident commander and reflect his action upon that information.

Some capabilities similar to those of CPOF are emerging in the commercial sector. MindTel has been developing situational merging technologies with displays to create optimized operational space visualization platforms. However, the information link is equally important. At a recent exercise in San Diego, a borrowed Navy airship was used to beam real-time visual "scenes" back to an analyst in what was called "street scene." During Operation Iraqi Freedom (OIF),

the Common Operational Picture or COP was transmitted simultaneously to 1000 vehicles 20-30 miles inside Iraq.

The National Interagency Fire Command Center (NIFCC) in Boise, Idaho, is an example of an all-source fusion center specifically designed for supporting incident command decision-making regarding the threat of forest fires. This fusion center coalesces complex data on logistics, personnel, operations and other support across multiple states and jurisdictions, acting as a fire information clearinghouse. For example, the Regional Fire Directors furnish a daily status reports during the fire season to the National Interagency Fire Coordination Center (NIFCC), and the NIFCC Coordinator fuses this to provide a daily summary, by region, of the fire danger and fire occurrence statistics, and distributes this to their Washington office, regions, areas, and requesting states. The NIFCC uses state of the art technology, to include broadband communications, to collect and disseminate visual products to enable command decision-making, and has a dedicated intelligence section that solely works issues related to fires.

Computer generated intelligent agents or, more appropriately, "intelligent software agents" are also an enabling technology. These agents are capable of recognizing certain conditions, reasoning about these conditions, forming conclusions, and taking actions on the basis of those conclusions. One example germane to All-Source Situational Understanding being developed through California Polytechnic University at San Luis Obispo, California, is EMERRS or Emergency Regional Response Systems.

In general, EMMERS is the emergency response version of this same intelligent agent approach, and is described as an integrated decision-support capability for enhancing crisis management and improving or expanding response. The EMERRS system design incorporates collaborative agents with knowledge in specific domains. Proactively mirroring changing circumstances, these automated agents send alerts, inferences, and recommendations to response personnel. Agents are used to gather and reveal information so that the user can have access to the most accurate and up-to-date information, accelerating the decision-making process and providing continuous support at all points in the decision-making process. These "agents" monitor and contribute solution strategies within their areas of knowledge.

Currently, EMERRS is an evolving collection of decision-support applications designed to assist urban response units in dealing with a wide range of crisis management situations. It is a collaborative toolset that monitors an urban environment and provides enhanced near real-time situational awareness to emergency response commanders and their staffs. Functionally, EMERRS integrates data from disparate sources into a single coherent view that provides a disciplined decision-making environment. Potentially, it enables the crisis management staff to minimize or eliminate time-consuming data filtering tasks. For the UIC, this allows greater resources and attention to higher-level situational assessment and rapid response to changing events. User requests for assistance are supported. However, the system does not wait for requests to offer contributions. EMERRS provides a decision-support environment in which agents and human users interact to solve problems collaboratively.

Technology Limitations and Barriers:

Bandwidth is again a huge limitation. Real-time video and the types of large data files involved with imagery, modeling and special GIS products will truly revolutionize how emergency responders communicate.

Developing intelligence agents is another issue addressed at the workshop, or more appropriately smart automated agents that can mine data and learn artificially. The potential of these is great, but so is the time needed to significantly improve the current technology to the point where it can provide truly smart agents. With the overwhelming amount of information available today, especially through the Internet, today's smart agents could end up funneling tremendous amounts of information to a human analyst or responder that would slow down their assessment or decision-making processes instead of streamlining and improving them.

Training of emergency personnel is another issue. There is tremendous software and hardware available, but the threshold of training that it may take to gain, let alone maintain, proficiency in using them is very significant. Current methods relying on on-the-job training or going to a course and then rarely using it won't work. The training must be made available and that will be expensive. However, it does play to one of the strengths of the Department of Defense and the rest of the federal government in that there is a powerful training capability available to address this need for the nation's responder community. This is especially true for areas dealing with intelligence support to the Unified Incident Command, since DoD is virtually the only organization that has training schools with course subjects and substantive experience or knowledge dealing with this requirement.

Gap Fillers:

Responders saw the development of common doctrine and processes across multi-jurisdictional, governmental and civil-military lines as critical. Once doctrine has been developed, there must be a corresponding systems integration effort that mirrors operational or intelligence doctrine.

All-Source Situational Awareness Response Technology Objectives (ASUrto)

ASUrto.1 – All-Source Information Fusion and Analysis System

Objectives:

Develop a prototype tool and doctrinal template for an information and analysis cell to support Incident Command. The objective is to evaluate, select and integrate technologies that will enable the capability to collect, fuse, analyze and present information from all sources, including sensitive intelligence information. The tool should provide analysts supporting Unified Incident Command with the ability to collect, mine, correlate, perform pattern recognition, and visualize large amounts of data in order to contribute to real-time situational awareness, predict threats and vulnerabilities, and foresee the impact of proposed courses of action.

The system should be able to provide analysts with access to information from agencies at the local, state and federal level, including intelligence agencies, when required. Therefore, it will need to be able to transmit and manage classified information appropriately at various levels. The intent is to develop a prototype suite of information and communications technologies and a doctrinal and procedural template for regional authorities to procure and implement to create this capability. This capability follows the philosophy of preparing for all hazards. It would be useful not only in terrorists' incidents but in any critical incident and perhaps on a daily basis in some regions.

The objectives of this RTO are very similar to those of the Homeland Security Command and Control ACTD in the Department of Defense. Therefore, it will be useful to leverage that program and wait to begin this RTO until the HSC^2 ACTD is completed. As this is a classic opportunity for spiral development, the program should be planned in a way that seeks to deploy a capability as early as possible with plans to upgrade the capability as experience with the system grows. The prototypes can then be used by local governments as a guide for implementing their own capability.

Payoffs:

This will provide incident command authorities with intelligence products (analyzed all-source information) with far more fidelity than is currently available. It would enable access to sensitive information previously not available to them because they could not handle sensitive information. It would greatly strengthen their decision-making by providing a better picture of the incident environment but also provide better analysis of the courses of action they are considering. In the long run, responders will be better prepared, incident commanders will make better decisions, lives will be saved and property damage mitigated.

Challenges:

The technologies to support the objectives of this RTO exist and many are commercially available. What is not commercially available is likely available in the Defense technology base. Integration of these technologies, some of which may be proprietary, is the technical challenge. Some of the most vexing technical limitations involve the same challenges found across the entire command, control, communications and information management spectrum: integration with legacy systems, communications capacity (bandwidth), and whether the communication and information management infrastructure can be made to support the multilevel security needs of processing intelligence. Scalability and quality of service requirements may also be a challenge. In addition, responders simply have little experience in moving information, especially intelligence information, around their community during a major incident. Federal authorities have concern about passing sensitive information to local and larger audiences. Overcoming cultural and policy issues with multi-agency information sharing will be a challenge.

Milestones/Metrics:

FY2006: Evaluate the Homeland Security Command and Control ACTD. Review the results and assess the applicability of the technology suite and other developments (*i.e.,* doctrine, techniques) to the objectives of this RTO. Begin development of the prototype architecture. Establish a concept of operation/doctrine development team. The team will review current information analysis and intelligence sharing techniques and protocols. The team will begin to develop standard doctrine and concept of operation for a responder all-source information analysis cell.

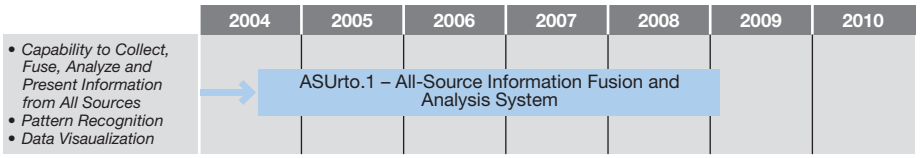
FY2007: Continue development of CONOPS and standard doctrine and procedures for information and intelligence support to incident command. Complete architecture and perform a gap analysis between the target technology suite and the HSC^2 ACTD. Determine how to fill the gaps either with emerging technology or new development. Select available technologies that will support the developed process and begin integration. Begin integration of initial capability prototype system, including the technology suite and CONOPS and doctrinal templates.

FY2008: Complete integration of initial capability prototype system. Begin testing of prototype system. Analyze test results and develop improvements in the technology suite and process templates based on test results. Demonstrate the prototype system in a major critical incident exercise.

FY2009: Begin deployment of the prototype system in several cities. Continue to integrate improvements in capability either through technology upgrades or improvements in CONOPS. Demonstrate new capability as appropriate.

ASUrto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	Totals
All-Source Information Fusion and Analysis System	$0	$0	$3.0	$5.0	$6.2	$4.0	**$18.2**



All-Source Situational Understanding Technology Roadmap

Chapter XII

Criminal Investigation and Attribution (CI)

Chapter Chair: Hal Kempfer
Chapter Coordinator: Dr. Maria E. Powell

Definition

Criminal Investigation and Attribution (CI) is the ability to rapidly, reliably and safely identify the perpetrators of suspected terrorism incidents, including the ability to collect, process, and examine the evidence, identify and interview witnesses, and determine the type, cause and initial location of an incident.

Operational Environment

This NTRO is focused on the five Operational Environments represented by threat: chemical, biological, radiological, nuclear, or high-explosive/incendiary (*i.e.*, CBRNE) effects of an event.

Needed Functional Capabilities and Priorities

Responders identified four functional capability elements they require for this NTRO, presented below in order of descending priority (as determined by responders).

- Management of Contaminated Suspects and Witnesses
- Contaminated Evidence Recovery and Preservation
- Coordination between Law Enforcement and Public Health Authorities
- Post-Incident Forensic Modeling and Simulation

Overall State of Technology for Criminal Investigation and Attribution

As the matrix below indicates, responders feel they have at least a marginal capability in most areas in this NTRO, with the exception of radioactive evidence recovery and preservation. Furthermore, the technologies that support this NTRO are available today for the top three priority functional capabilities. The fourth-priority capability, *Post-Incident Forensic Modeling and Simulation* (CI.4), relies on technologies that are marginally available in the near-term, except in the biological operational environment: in this environment, the technologies are high-risk and not available in the near term.

Criminal Investigation/Attribution

Functional Capabilities	Operational Environments: Chemical	Biological	Radiological	Nuclear	High Explosive/ Incendiary
1. Management of Contaminated Suspects/Witnesses					
2. Contaminated Evidence Recovery and Preservation					
3. Coordination Between law Enforcement and Public Health Authorities					
4. Post-Incident Forensic Modeling and Simulation					

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

CI.1 – Management of Contaminated Suspects and Witnesses. *The ability to quickly identify,*

quarantine and decontaminate potential suspects and witnesses, and interview and process them.

Goals:

- Quickly identify and segregate suspects from witnesses, in quarantine facilities.
- Integrate, sustain and equip (with proper PPE) law enforcement personnel within decontamination process, so they can have the ability to observe and interview during decontamination process.
- Every patrol officer outfitted with quickly adaptable Level C PPE specifically designed for their use, to apprehend suspects and interview if no time for decontamination (including knowledge of contaminant and/or symptoms of victims). (See Chapter II (PPE).)
- Pre-positioned or ultra-light PPE for foot patrol officers (multi-purpose uniform).
- A checklist for immediate action to assess the situation and provide for better and safer response.
- Track individuals who were decontaminated or processed (facial recognition, photo/video, etc.).

Current Capabilities:

Responders have this capability today in high-explosive or incendiary environments, but there is a marginal capability for emergency responders in most communities to conduct interviews or interrogations in a warm zone (*i.e.*, with chemical, biological, or radiological contaminants). Handling contaminated witnesses or suspects relies on the same capabilities as handling contaminated general populations. These capabilities were discussed in earlier chapters (especially Chapter II (PPE)). Finally, responders have (or have access to) capabilities for stand-off interviewing/interrogation such as closed-circuit television: the challenges here would be more from criminal procedure and legal requirements rather than technology.

An important issue is the need to assess the situation quickly during a CBRNE incident. This involves some use of technologies such as sensors, imaging equipment and wideband connectivity. Whereas smaller jurisdictions may not have on-hand all of the PPE and decontamination capability they need, they may be able to develop and disseminate an accurate picture of the contaminated area, and then virtually be supported in designating a hot/warm/cold zone. Thus, this functional capability is inherently dependent on capabilities described in Chapter III (DIDA).

Responders noted that there is a shortage of facial recognition capability useful for tagging suspects or other persons of interest. Other technologies might be more useful to collect and retain biometric data for identification use at a later date, such as iris scans, or technologies from programs such as DARPA's Human Identification from a Distance (HID). Nevertheless, most of these capabilities are not present in most responder jurisdictions.

State of the Art:

Technologists identified virtual or automated means for identifying and tagging suspects or persons of interest. Amongst the ways of tagging suspects is facial recognition or some other biometric identification means. Currently, law enforcement is using finger and palm prints for identification of suspects, and casinos have been widely adopting facial recognition technology for tagging suspects within the gambling industry. These technologies are useful for managing suspects in a contaminated environment. These technologies are also useful for identifying and distinguishing witnesses among crowds.

Biometric technologies are also useful in cases when contaminated suspects must be interviewed from a distance, for example, using isolation and closed-circuit television. Responders noted that only California can conduct interviews of contaminated suspects, and federal resources are needed to help with this issue. The FBI has HAZMAT teams that are trained and equipped for crime scene investigations in contaminated

areas, to include interviewing contaminated suspects. There are technologies that ensure identity through biometrics sufficiently for legal purposes.

It has been said that the casino industry is "pushing the envelope" of technical innovation in visual and behavioral surveillance. Modern developments in closed circuit television (CCTV) and video recording technology have become methods for uncovering crime as it is taking place and providing an archived record for later investigative action. Breakthroughs in digital imaging technology, especially regarding facial recognition, have created the public impression that casinos are much farther ahead in this area than other industries. For example, the Trump Marina Casino in Atlantic City, NJ, claims to have 10,000 photographs of cheaters, and people who have been arrested, evicted or ejected from their or other casinos, for use in their facial recognition system.

Responders identified the need for fusion of pre-existing databases for suspect management and record correlation. There is also a need for immediate fusion and correlation of interview and investigative data, with the added capability of providing logical leads and dynamic investigative decision modeling in near-real time. With improvements in imaging technology, wireless internet service, and personal communications and information devices, the ability to input, query and receive data from pre-existing databases while in the field is becoming less of a technology hurdle. In most cases, this technology already exists and it is only matter of funding and political will to test and evaluate it, and deploy it in the field.

Technology Limitations and Barriers:

The technology to provide this capability is available today, across all of the operational environments. Technology limitations to providing this capability are mainly interoperability (to fuse communications between hot zones and other responder locations) and portability (for example, getting equipment for contaminated witness interview or suspect questioning into a hot zone). Otherwise, the technology limitations are similar to those in Chapter III (DIDA); that is, knowing about the presence of hazards and the parameters of the hot and warm zones.

Gap Fillers:

Since technology is relatively mature, no gap fillers were considered.

CI.2 – Contaminated Evidence Recovery and Preservation.

The ability to collect, process and preserve potentially contaminated evidence (to include devices and fragments), in a contaminated environment while ensuring chain of custody.

Goals:

- Process contaminated fatalities.
- Secure separate storage facility for custody and examination of contaminated evidence.
- Tracking of evidence that supports the chain of custody.
- Contamination control for selective decontamination without cross-contamination tools that do not destroy evidence.
- Safe transportation and containers for contaminated evidence to include contaminated corpses.
- Remote or stand-off devices for collection of evidence.
- Easily decontaminated or disposable processing tools for all of the above.

Current Capabilities:

Responders have this capability in the high explosive and incendiary environments. This capability is marginal in the biological and chemical environments, and is non-existent among most responder jurisdictions for the nuclear and radiological environments.

Collection and preservation of evidence is critical to responders. Much evidence is collected after incident, but contaminated evidence poses challenges in transporting, analyzing, and using it for evidentiary purposes. This is an issue of expertise

and training as much as it is an issue of technology.

Responders generally rely on clear plastic bagging for sending contaminated evidence out of hot zones. One notable exception is a corpse or human remains, which are still wrapped and sealed so to avoid contamination.

Forensic standards for bioagents are not well established, either in law or practice. This is an area that is still evolving, and the anthrax attacks following September 11th may eventually provide lessons or direction that can be used to shape the appropriate technologies needed for forensic trace-back. In addition, state courts (and thus, local responders) will probably look to federal legal experience, procedures, and case law when applying forensic standards, in the event a terrorist attack would be a subject for state courts. Much will be learned from the use of the Daubert test and the introduction of new technologies and procedures at the federal level.

Responders have marginal capability to collect bioagents as evidence. The technology to do this has been bulky, expensive and not widely available.

For secure storage of contaminated evidence (for custody and examination), it is unlikely that the expertise and capabilities to exploit the evidence fully (including for leads) will exist in sufficient quantity and quality to perform these analyses and examinations, without federal help and intervention. Some of the expertise already exists (*e.g.*, identification of microorganisms) within the state and county public health laboratories. However, this expertise does not extend to the forensic analysis and investigation of the event. Virtually all of the forensic expertise and capability related to these events resides at the federal level. Unique sets of complementary expertise reside in various components of the federal government (with help from a select group of consulting experts, some of whom are at the state, local or university levels).

State of the Art:

Technologies exist for connecting contaminated samples from hazardous buildings. Samples contaminated by biological and chemical agents (or when sampling the agents themselves) usually requires secure transport of the samples to a laboratory for final composition analysis. While there are only a few "Gold Standard" laboratories in the country that can make a 100% accurate identification, there has been an increase in the number of "Silver Standard" laboratories that can make a 90-99% accurate identification. In the last two years, a number of the field-deployable National Guard Civil Support Teams (CSTs) have added this silver standard laboratory capability. It should be noted, however, that the application of these standards is usually for identifying a biological agent and its characteristics, rather than necessarily identifying the origin of a biological agent for forensic attribution purposes. The two applications are related, but not distinct, and require different standards of effectiveness.

Another application for biometric technologies is handling contaminated evidence. This includes "triage tags" for contaminated items, to include evidence tags. With current commercial technology, it is possible to image any piece of evidence in the hot zone prior to it being moved, and thus create a visual tag. Potentially, this could be linked with other automated means of "tagging" that could minimize the amount of manpower involved with collecting and tagging evidence.

The FBI's Hazardous Materials Response Unit and the FBI Laboratory have spent years developing capabilities and procedures for collecting, preserving, and the administrative handling of contaminated evidence. Furthermore, the FBI conducts training for responders, especially HAZMAT and WMD response teams, on issues regarding preservation of evidence. Saving lives continues to be first priority for responders. However, sensitizing responders to criminal evidence issues and collection requirements can help to avoid unnecessary damage to the forensic value of potential evidence. FBI procedures are to bag

the evidence in the hot zone, and then "double-bag" it. The outer bag is then decontaminated in the warm zone, and the evidence bag is tagged in either the warm or cold zone by an Evidence Response Team Technician, who then preserves chain of custody. Tagging evidence in the hot zone is not something easily accomplished now.

On some occasions, it might be necessary to capture images of the crime scene as rescue operations begin, in order to capture the visual evidence of what the scene looked like prior to responders conducting operations there. Even if physical evidence is moved, an imaged scene allows investigators to recreate where certain pieces of evidence were in relation to the original layout prior to recovery operations, and then put this together for potential criminal prosecution later on. Furthermore, it might be important for juries and judges to visualize the evidence in context of the scene of the crime. Current technology can be used to portray the crime scene safely in court, using robotics, aerial reconnaissance (unmanned or manned), CCTV, etc. Taking lessons from the imagery intelligence (IMINT) community, it is possible to develop extensive analyses using imagery of what happened. Responders noted that using robotics is clumsy, but is sufficient to ensure chain of custody in order to meet rules of evidence.

Technology Limitations and Barriers:

The technologies are basically available today to provide this capability, with some challenges. Occasionally the decontamination process destroys evidence. Contaminated objects cannot be entered into evidence or handled and stored in the same way as uncontaminated evidence. Traditionally the court questions the chemical alteration from compounds or added surface deposits due to the decontamination process. Attorneys will argue about what was done to "decon" the evidence, and how this may have compromised its forensic value.

Gap Fillers:

Technologists have noted rapid improvements in bio-genomics, which are useful in the development of forensics biological databases. Potentially, this can improve the process of determining origins of biological samples.

CI.3 – Coordination between Law Enforcement and Public Health Authorities. *The ability to coordinate among law enforcement, public health authorities and medical examiners/coroners, for epidemiological surveillance, information to support attribution (and vice versa), to include fusing epidemiological surveillance information from public health with law enforcement epidemiological evidence.*

Goals:

Provide evidence and analysis to law enforcement, supported by the documentation, and within the parameters by which law enforcement receives notification of epidemiologists' observations and conclusions.

- Receive and interpret epidemiological information to support the investigation.
- Provide evidence and information to epidemiologists to support their efforts.
- Automate alert and cueing system supporting two way information flow between law enforcement and medical examiners.
- Standardized and interoperable technologies and mapping, information sharing, etc.

Current Capabilities:

This capability is marginally available today to emergency responders in the chemical, biological, and radiological operational environments. This functional capability is not relevant to the high-explosive/incendiary and nuclear (*i.e.*, blast effects *per se*) operational environments.

Much of this functional capability is dependent upon coordination between law enforcement authorities and public health/epidemiological officers. This cooperation exists today. However, automation would greatly enhance this functional capability.

State of the Art:

The CDC has funded several new labs that fuse information between hospitals and law enforcement. For example, in April 2003, the CDC opened the new Marcus Emergency Operations Center, a facility that improves the agency's response to health crises and enables faster and more coordinated response to public health emergencies nationally and worldwide. It has communication links with the Department of Health and Human Services, federal intelligence and emergency response officials, the Department of Homeland Security, and state and local public health officials.

The Syndromic Surveillance System is a benchmark of current capabilities, including some technologies that enable automation. Its data focus and staff includes:

- Epidemiology
- Health Planning
- GIS/Mapping
- Administrative Coordination

By May 2003, the CDC estimated that state and local health departments have begun syndromic surveillance systems in about 100 locations around the country, with the goal of earlier detection of epidemics and faster public health response (*i.e.*, from days to hours).

The Los Angeles County Terrorism Early Warning Group (TEW) has an epidemiological intelligence ("epi-intel") team that monitors health service information for indicators and warning of a potential outbreak. Responders noted that bio-information needs to tie into investigations for quickly finding the perpetrators, and then removing them from further threat and hopefully deriving valuable information to help mitigate the current threat. The LA TEW does this by directly linking epi-intel into terrorism investigation groups through its investigative liaison office. TEWs are being established in a number of cities nationwide, especially on the East and West Coasts.

TEW and the HHS Metropolitan Medical Response System (MMRS) are state-of-the-art practices, as opposed to technologies. MMRS enhances the capabilities of existing systems that involve hazardous materials, law enforcement, and emergency medical services personnel, public hospitals, and the American Red Cross, as well as public health agencies and laboratories, private hospitals, clinics, independent physicians, and other private-sector organizations. Over the last six years, HHS has established contracts with 122 cities. HHS provides the cities with funding for special equipment and pharmaceutical and medical supplies, and in return, HHS requires cities to provide detailed plans on how the city will organize and respond to chemical, biological, or radiological agents.

Technology Limitations and Barriers:

Technologies in support of this functional capability are available today, including information technologies that would automate information sharing. Primary limitations and barriers are cost, organizational, or, in some cases, political and legal. For example, responders noted that if the syndromic information is collected in hospitals, the technology readily exists to flag it for dissemination to law enforcement, but the question of compliance with privacy laws is not necessarily resolved. A good deal of the medical data sources routinely collected for other purposes, such as emergency room logs, pharmacy sales, school absenteeism, etc. can be fused and analyzed for spotting emerging trends. There is legal concern about this though, since this is not generally something done by health departments.

Responders noted that law enforcement officers need basic training in the "epi-intelligence" process. This is not a traditional area of standard law enforcement training curricula, either at the academy level or advanced training.

Gap Fillers:

There are already extensive law enforcement and public health communications and information systems already in place; responders and technologists agree that a critical gap filler is simply

expansion of existing systems. In addition to expansion, information flows in these systems need to be two-way: health authorities need to be sensitized and responsive to law enforcement and public security issues, and law enforcement must be equally sensitive to the needs of the health services community.

CI.4 – Post-Incident Forensic Modeling and Simulation. *The ability to reconstruct and analyze the incident, to support inferential evidence, and to support investigation and prosecution.*

Goals:

- Models that support analysis in three dimensions, and take into account environmental conditions such as atmospheric, humidity, etc.
- Portable (for responders) laptop systems to document and gather data at incident site to use as inputs for the model.
- Reconstruct passage of events.
- Automated playback of events.
- User-friendly, low cost, and easily upgraded.

Current Capabilities:

This functional capability is marginally available to responders today, mainly because of cost limitations. Technology exists to support this capability today to a limited extent, but tends to be prohibitively expensive and only large jurisdictions can afford it.

Forensic modeling and simulation are critical objectives for responders. They represent the ability to "see" what has happened or is happening respectively on the ground regarding CBRN contamination or effects. Forensic modeling is far more detailed than simulation modeling, and probably less defined in some respects, because it is potentially used for evidentiary purposes and not just to enable operational decision-making. For example, the wildland fires in Southern California in Fall 2003 exhibited what can happen when those managing a dynamic series of very large, destructive incidents cannot predicatively "model" what is happening or going to happen. Since it is unknown if some of these fires are related to terrorism, causality could be assumed either way regardless. With that said, there are many good fire prediction modeling software applications available, but the results of the fires speak for themselves. With nearly 3000 homes destroyed, sixteen lives lost and over $2 billion in damage, there is now the problem of creating a detailed forensic model that can help investigators determine causality and, eventually, culpability.

State of the Art:

There exist several plume modeling programs (notably those developed by the DoD Defense Threat Reduction Agency and the Department of Energy), but within these programs there is still the need to add the fourth dimension of time. These models have various strengths and weaknesses, but as static constructs, their utility diminishes over time as contamination areas shift with weather and other factors.

Various laboratories have been developing methods for early detection and rapid treatment. For example, universities in New Mexico have formed a consortium with Los Alamos and Sandia National Laboratories and the New Mexico State Department of Health, to develop a model for population surveillance using real-time reporting by health professionals in emergency departments of any patients reporting flu-like symptoms. These technology efforts can be applied to forensic modeling.

Technology Limitations and Barriers:

The technologies to provide forensic modeling are marginally available in the near term, and are of medium technology risk for development, for all operational environments except biological threats. For the biological operational environment, the technology is not available in the near term, and development of the technology faces high development risk. In addition to the limitations described below, technology in this area will face many of the same challenges inherent in detecting, identifying, and assessing threat agents

(see Chapter III (DIDA), for a discussion of these challenges). This functional capability relies on many of the capabilities described in Chapter III.

Most models today have limited model validation and certification, with no centralization. This undermines their effectiveness for forensic modeling. Many models rest on data that is either outdated or limited in the range of threat agents. Modeling systems work well for anthrax but not others. Models that function for chemical weapons do not work well for toxic industrial chemicals/materials, and vice versa. In many cases the working models or projections rely on outdated, obsolete data. Biological models are especially problematic in their underlying data, as there are few effective simulants for the models, and thus the models cannot be tested for effectiveness short of actual deployment in a real attack. There is a need for new models and adaptive models that can be tailored to specific urban environments and fused with other datapoints (*i.e.*, terrain, population, meteorological input, etc.). Furthermore, many models are limited by data entry and human factors issues: to be more effective, forensic models must have automated data entry (*i.e.*, tied to agent and environmental sensors), and be more user friendly.

Models are also undermined by a poor understanding of incendiary physics (especially thermobarics), fate and effects for biological agents, and effects from combinations of agents in attacks. This lack of comprehension undermines the analytical basis and thus accuracy of models.

The effects of chemicals and biological agents dispersed in urban or complex terrain are difficult to model effectively with current technology. DoD modelers for U.S. Northern Command's exercise "Determined Promise '03" had to manually alter models to reflect urban terrain, environmental impacts, and "micro-climates" of the Strip area of Las Vegas. Several research projects are underway, but there is still no software package available that can automatically adjust for this complexity. In particular, biological models are the highest risk for technology development. In addition to the above limitations and barriers, it is inherently more difficult to model for contagion.

Gap Fillers:

There is much data in the federal government (especially DoD) that could be used to enhance or update the underlying data sets of existing models. Added data sets needed in these models include inputs for microweather variations found in vertical terrain, such as urban areas. In addition, "After Action Reports" on public health or terrorist events, notably the October 2001 anthrax attacks, can be useful for strengthening existing models' data sets.

Note: Responders and technologists felt that the critical technologies supporting this NTRO are being proposed in other NTROs, principally Chapter II (PPE), Chapter III (DIDA) and Chapter IV (UIC). Therefore, no Response Technology Objectives are offered here.

Chapter xiii

Mitigation and Restoration for Plant and Animal Resources (MRPA)

Chapter Chair: Dr. Thomas W. Frazier
Chapter Coordinator: Dr. Maria Powell

Definition

Mitigation and Restoration for Plant and Animal Resources is the ability to prevent or mitigate, detect and neutralize damage to plant-life, animals (*i.e.,* wildlife, livestock, exotics, pets and other domesticated animals), food, feedstuffs, and humans caused by a terrorist event aimed at agriculture and human and animal health.[14]

In line with the Project Responder emphasis on responders, this NTRO leaves out many important elements of plant and animal resource protection. For example, research on novel vaccines and prophylaxis (as opposed to responder delivery of these medicines), and developing resistant strains of plants and animals, are outside the scope of Project Responder.

Operational Environments

Mitigation and Restoration for Plant and Animal Resources occur in six operational environments: Animal, Plant, Human Health, Food Processing, Food Distribution, and Feedstuffs. Rather than restricting animal and plant environments of present concern to livestock and crops, it was concluded that there should be a wider perspective that would encompass animal wildlife, insects, weeds, flowers and decorative plants. While these may not be the focus of catastrophic terrorism, they reflect the very broad scope of the food and agriculture sector and the activities and resources it involves. Feedstuffs are of concern because of previous deliberate contaminations of animal feed with toxic substances like insecticides and dioxins, and because the incorporation into animal feed of central nervous system materials carrying bovine spongiform encephalopathy (Mad Cow) disease has had such a devastating effect on the English beef industry and is currently the cause of an embargo on Canadian beef. Food processing and food distribution are also distinct environments with different methods for surveillance, detection and decontamination. Human Health is called out separately as an operational environment to ensure adequate consideration of the effects of vector borne and zoonotic diseases that are transmitted to people.

In contrast to the other NTROs, although in some instances firefighters and law enforcement personnel may be pressed into service to protect plant and animal resources, the first line of defense will be extension agents, employees of state departments of agriculture and natural resources, veterinarians, forest rangers, and similar professionals.

Needed Functional Capabilities and Priorities

Responders and technologists considered a set of eight functional capabilities to handle the operational context described above. These capabilities are presented below in order of descending priority:

- Rapid Diagnostics and Detection to Confirm the Introduction of CBR Agents to Animals, Plants, and Food/Feed

[14] The MRPA NTRO evolved from the Agricultural Mitigation and Restoration NTRO that was discussed as being under development in the March 2003 Project Responder Interim Report, *Emergency Responders' Needs, Goals and Priorities*.

- Coordination of Animal and Plant Entities with Public Health, Law Enforcement, and State, Local, and Federal Government and Industry
- Identification of Outbreak Origins and Spread
- Animal and Plant Diagnostic Surge Capacity
- Vaccination/Treatment and Protection
- Quarantine, Isolation and Recall
- Rapid and Humane Euthanasia and Disposal of Contaminated Carcasses, Plants and Food Products
- Decontamination

It should be noted that under directives for Awareness and Warning, Mitigation Strategies, Response Planning and Recovery, Outreach and Professional Development, the Homeland Security Presidential Directive/HSPD-9 *Defense of the United States Agriculture and Food*, January 30, 2004, touches upon a number of issues subsumed under these functional capabilities. HSPD-9 establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

Overall State of Technology for Mitigation and Restoration for Animal and Plant Resources

The matrix below presents a mixed picture of the current and near-term availability of needed technologies and the degree of technical risk associated with developing and fielding the needed capabilities for the future. For rapid diagnostics and detection technology needed to confirm a CBR incident, the technologies needed to achieve the desired level of capability do not yet exist. By contrast, capabilities for organizational and technical communications networking needed to coordinate remedial action are lacking but the technology to support these capabilities is readily available.

Technology for determining outbreak origin and spread generally exists, but is not operationally available to emergency responders in the animal, plant, or human health areas. For food processing, food distribution and feedstuffs, the technology is commercially available and used in practice. Similarly, the animal and plant agriculture communities have yet to establish functional cooperative relationships for meeting surge diagnostic needs, although the technical capability to do so exists. The human health, food processing, food distribution, and feedstuffs areas are better prepared to meet surge capability needs and have procedures and technology in place to do so.

The *Vaccination/Treatment and Protection* (MRPA.5) ratings reflect that the technology generally exists, but is not operationally available to

Mitigation and Restoration for Plant and Animal Resources

Functional Capabilities	Operational Environments: Animal	Plant	Human Health	Food Processing	Food Distribution	Feedstuffs
1. Rapid Diagnostics and Detection to Confirm Introduction of CBR Agents	1	1	1	1	1	1
2. Coordination of Animal and Plant Authorities with PH, LE	3	3	3	3	3	3
3. Identification of Outbreak Origins and Spread	1	1	1	2	2	2
4. Animal and Plant Diagnostic Surge Capability	3	3	3	3	3	3
5. Vaccination/Treatment and Protection	1	1				
6. Quarantine, Isolation and Recall	2	2		2	2	2
7. Rapid and Humane Euthanasia and Disposal	1	2		1	1	
8. Decontamination						

1. Do emergency responders have the functional capability in this operational environment? YES / MARGINAL / NO
2. Are technologies available in the near-term to provide this functional capability? YES / MARGINAL / NO
3. What are the technology risks of developing this functional capability? LOW / MEDIUM / HIGH

Gray coloration signifies 'Not Applicable.'

meet the challenges of some potential attacks involving relevant chemical, biological, or nuclear threats. Relative to the overall readiness of vaccines and alternative treatments to meet the full threat spectrum, a "red" rating could have been justified. (The Project Responder focus is not on the availability of vaccines and treatments but the availability to responders of the means to administer them.)

Quarantine, Isolation, and Recall (MRPA.6) technology is also relatively available to emergency responders, although the capabilities would not be fully adequate for catastrophic incidents involving large numbers of animals or large growing areas. The same applies to rapid and humane euthanasia and disposal of contaminated carcasses, plants and food products. The technology exists, although it could be improved. It is not immediately available to emergency responders in agriculture and they would need orientation and training for using it in emergency situations.

Contaminated animals and plants are usually destroyed rather than decontaminated. The same applies to feedstuffs. Technology for decontamination of food processing and distribution facilities exists. Emergency responders who work in these settings are familiar with its use and have access to it.

MRPA.1 – Rapid Diagnostics and Detection to Confirm the Introduction of CBR Agents to Animals, Plants, and Food/Feed. *The ability to either run a field test, or a more definitive test at a state or regional laboratory, and to perform aggregation and analysis of the results.* This capability includes ongoing surveillance and rapid detection of chemical contaminants, pests, pathogens, toxins, and adulterants (known and unknown). Field capabilities should include software-assisted syndromic evaluation of animal or plant symptoms and signs as well as testing of specimens. Overlapping or similar capabilities are addressed in DIDA.1 (*On Scene Detection*), DIDA.3 (*Classification and Mitigation*), MR.4 (*Rapid Clinical Environmental and Veterinary Field Assessment*), PHRBAE.1 (*Surveillance and Information Integration System*), and PHRBAE.2 (*Rapid, High-Throughput Clinical Assessment and Testing*).

Goals:

- Rapid (*i.e.,* 15 minute-test) field diagnostics for use by emergency responders are critical.
- Reduction of the time between pathogen introduction and response.
- Adequate field instrumentation to both detect and identify chemical contaminants, pests, pathogens, toxins, and adulterants.
- Lab tests to identify genomic components.
- Rapid laboratory identification and verification of highly contagious diseases that require immediate attention and drastic actions as opposed to those conditions with similar symptoms (high sensitivity and specificity).
- Education, training, and equipping staff in identification and sourcing, of potential front-line responders (including producers) to know what to look for, whom to contact, appropriate procedures, and incentives to report potential threats.
- Adequate stocks and distribution of diagnostic reagents and resources (cells, primers, tests, reagents, etc.) with long shelf lives.
- Surveillance grid that is automated and active for remote plant and animal disease surveillance to indicate deviation from baseline within 4-6 hours (for animals) twenty-four hours (for plants) and four-six hours (for food processors/distributors).
- Standardization of diagnostic methods, and instituting an accreditation process for diagnostic laboratories.
- Improved techniques for screening bulk containers (including ships, barges, trucking and railcars) and methods to screen and analyze foods/feedstuffs.
- Redundant laboratory capabilities, able to manage nationally distributed/multi-target incidents and handle varying levels of biological materials; good workability between public and private industry reference laboratories.

- Identification and testing for prodromal state/onset of symptoms based on behavioral and/or physiological parameters/signs in real-time.
- Access to animal and plant disease databases with reference images, which includes diagnostic test procedures available for pathogens and where they are performed; contact information for scientific experts by disease agent; and plant and animal pathogen/pest information for initial identification.
- Mobile laboratories suitable for Biosafety Level 3-4 disease management and analysis for field use, so that specimens don't have to be trucked to the laboratory.
- Real-time detection and analysis capability for viability and disease potential assessments.

Additional Considerations Regarding Goals for MRPA.1:

- Many (especially plant and insect) exotic diseases are not widely known by American field personnel, suggesting the need for visually rich electronic field diagnostic aids and tropical disease networking with foreign laboratories and state and private sector laboratories.
- Field tests are needed for prohibited adulterants, antibiotics, hormones, and genetically modified varieties.
- Testing capabilities should include tests for biological toxins, which may be the main way that a pathogen attacks a host.
- Rapid diagnostics capabilities also need to include capabilities for testing dead animals which many screening tests cannot do.
- A complete rapid diagnostics capability should include field screening tests that can help emergency responders avoid exposure to pathogens (especially viral) agents that might be dangerous to them, including protective gear for use while making these determinations.
- Special emphasis needs to be placed on technology transfer and human engineering activities concerned with transforming laboratory tests into field analyzers suitable for use by relatively untrained emergency responders and producer staff.
- DIDA surveillance capabilities should include monitoring of water and air for pathogens and chemical contaminants of concern to plant and animal health.
- Wildlife biologists and ornithologists should be considered emergency responders.
- Weed analysis tests are also needed since weeds can be most destructive to plant crops.

Current Capabilities:

There is limited understanding of the baseline data to adequately differentiate between what is normal and what is not. Current screening tests don't apply to all animals/species or all pathogens, since some remain either unknown or poorly studied. However, analytic capabilities are better for most chemical contaminants than for pathogens.

There is no rapid high through-put diagnostics. State and local jurisdictions lack facilities, high volume sample processing potential and adequate staffing for emergencies. While all State diagnostic facilities have ELISA (enzyme-linked immunosorbent assay) test capabilities, only some have PCR (polymerase chain reaction) tests for a limited number of pathogens only There is also an insufficient number of national reference laboratories; currently, there is just Plum Island (New York) and the Ames (Iowa) USDA Centers.

Currently, veterinary diagnostic laboratories routinely handle many pathogen analyses and could substantially increase surge capacities if necessary. For classical pathogens, veterinary laboratories already undertake a great deal of pathology and operate successfully under an established self-accreditation system under the American Association of Veterinary Laboratory Diagnosticians (AAVLD).

State of the Art:

One approach would be to monitor the environment for pathogens before they become endemic in flora and fauna. As discussed in Chapter III (DIDA) and Chapter VIII (PHRBAE), there are a host of detection strategies for biological agents, but each has significant limitations. Such surveillance systems must be automated with little need for user intervention or servicing. BW agents need to be identified at extremely low concentrations in complex, changing backgrounds, in near real time and with low power requirements and no reagents. Clearly, existing systems do not meet the needs well. They suffer from relatively poor sensitivity, occasional false positives, and lengthy response times. Good detection equipment would deter the use of such weapons by reducing an attack's effectiveness and increasing the probability of detecting the perpetrator. However, improved detection systems would present a host of positive spin-offs, such as in medical diagnostics, environmental monitoring, food and beverage processing, and product tracking.

Despite a multitude of ongoing and proposed development efforts on systems to meet Rapid Diagnostics and Detection to confirm the deliberate introduction of CBR agents to Animal, Plants, and Food/Feed, this technology remains still far from where it needs to be in meeting homeland security needs. This large gap exists across all the relevant operations environments reviewed. This combination of overall significance of MRPA in the face of a relatively early point in the state of the art supports making a major funding investment in these detection strategies, tools, and analytical systems at both basic and applied research and development levels of the systems development process.

A variety of federal agencies are now addressing these pressing, high-priority needs for rapid diagnostics and detection equipment to confirm the presence of CBR agents in these different operational environments. Some of the programs of early particular note include:

- DARPA programs: TIGER and on-chip technology
- Navy/DLA: food perishability tracking (smart-tags)
- Coast Guard/DHS: container inspection
- NASA: Satellite imagery for plants/crops/forestry
- Nano-fabrication (existing for chemical baselines and now being worked on in biologics) to get protein profiles as the baseline for detection
- FDA: food container inspection
- Commercial program initiatives: Wal-Mart program for tracking food processing and distribution
- Food safety inspection programs at University of Maryland, College Park's FDA lab, the FDA Food Safety Lab (Chicago), and the FDA Center for Food Safety and Applied Nutrition
- Los Alamos National Laboratory program on high-throughput diagnostics labs
- Genomics research and data for setting baselines and distinguishing between pathogens/adulterants
- Work in progress on gas chromatography for plant/animal studies
- The National Seed Health System (NSHS) works to implement diagnostic methods that have been evaluated and proven to be accurate, reproducible, and capable of detecting pathogens at a defined level of sensitivity; also conducts research in the development and standardization of seed health testing methods.

Technology Limitations and Barriers:

A variety of different technology limitations and barriers limit progress in developing and introducing rapid-diagnostics/detection systems for confirming introduction of CBR agents in the food and agriculture sector.

There have been substantial advances in technology for important biological agents, but they

have often not included agriculturally important pests or pathogens, nor have they been inexpensive or field-deployable. PCR-based tests cannot be used for newly emerging pathogens or novel genetically engineered pathogens/agents. Thus it is desirable to develop approaches oriented toward identifying classes of related agents. Genomics has potential to provide such screening tests, but contemporary knowledge of genomic structures and functional genomics for plant species, pests, and pathogens is very incomplete. Knowledge of functional genomics is actually still in its infancy. Analyzer technology cannot compensate for this deficit in basic knowledge. The great majority of plant species, for example, still remain to be subjected to genomic study. The same limitations exist for pathogens and pests, especially those associated with foreign plant disease. Prions too remain poorly understood.[15]

Another source of limitations and barriers relates to funding abilities and incentives of the private sector for new technology development in the absence of commercial demand. Once a new disease has become established, then a market will be created for such diagnostic equipment. For some threat agent that has not been experienced, however, the private sector will not invest capital for development in the absence of return on this investment.

An associated barrier has to do with sharing intellectual property. Researchers and R&D companies that have developed genomics information or other related kinds of information consider this information proprietary. Some charge fees to access genomics databases, for example. Other companies will simply not divulge this information.

Other financially related barriers include difficulties private sector and state laboratories experience in meeting overhead costs during austere times and associated collapsing infrastructures, maintaining program continuity, and recruiting and keeping talented scientists and technologists in uncertain times. Recruiting foreign national scientists and technologists has become an increasing problem because of new immigration and national security restraints placed on these professionals from particular countries.

An associated problem is that laws and regulations associated with biosecurity RDT&E are in an evolutionary period at present.

Gap Fillers:

Considering the present state of flux in agency missions, budgets, state and private sector initiatives and perceived vulnerability of the food and agriculture sector, two broad initiatives are important. These initiatives have to do with: (a) continuing productive basic RDT&E programs that need funding continuity and expansion; and (b) expanding national capabilities in personnel and institutional resources to build operational capabilities for surveillance and detection.

Past these broad institutional directions, an SRA and two RTOs have been identified to fill the identified gaps. As described in the Introduction (Chapter I), the SRA on biomarkers includes a focus on markers of CBR exposure in plants and animals; MRPArto.1 (Plant and Animal Responders' Decision Aid) addresses the responder need for a portable decision aid to help interpret signs and symptoms, to guide further information acquisition, to facilitate reach-back to additional expertise, and to suggest mitigation course of action; and MRPArto.2 (*Field Screening and Assessment Tests*) addresses technologies for rapid screening and testing of plants and animals for exposure to and contamination/infection by threat agents.

MRPA.2 – Coordination of Animal and Plant Entities with Public Health, Law Enforcement, and State, Local, and Federal Government and Industry. *The ability to bring together full power of local, state and federal emergency management and supporting agencies, as well as private industry-civilian intelligence, on a plant/animal/food event.*

Goals:

- Access to common (shared and standardized) communication devices and integrated (shared

[15] Prions (improperly formed proteins) are the causative agent in Mad Cow and related degenerative diseases of the central nervous system.

and standardized) data systems is essential for emergency responders.

- Intelligence agencies including private ones should be included in coordination efforts.
- Legal authority to protect both security and commercial sensitive data and to share data (surveillance, health alerts and response data) – needs to be considered as a national security resource; national, state and local levels; government/public safety sensitive.
- Incentive structure to encourage industry participation in information sharing.
- Integrated and coordinated mechanism or platform for a shared database or e-warning system; needs to include the ER community.
- Interface with a national/state hotline for plant/animal/food incidents.
- Better awareness of threats to the food and agriculture sector by the law enforcement community (especially rural), producers and industry.
- Establishment of diverse cooperator and stakeholder relationships with worldwide, national, state, and local agricultural entities, industry through joint programs and regulatory framework initiatives; to include consequences/ understanding of international trade implications.
- Ability to establish a two-way information flow between plant/animal specialists and human epidemiological surveillance activities (See PHRBAE.1 (*Surveillance and Information Integration System*)). Currently, plant/animal specialists do not have access to human epidemiological surveillance information.
- More effective communication systems (other than conference calls) to discuss incidents; broadly distributed peer communication system; secure and redundant.
- Smart distribution of information to include industry.
- Multi-agency command (MAC) on the national level; interagency work group at the federal level.
- Tailored emergency response task force that can be activated in a matter of hours that is pre-established and composed of government, industry, and academia.
- Integration into federal, state, county and local, emergency management and incident command systems as well as private industry (Infraguard[16] and existing Information Sharing and Analysis Centers [ISACs]).
- A single ISAC from food production through processing to consumption.
- Integration into Incident Command System.

Current Capabilities:

A study by the National Research Council[17] concluded (2003) that coordination amongst federal, state/local and private entities appears to be insufficient for effectively deterring, preventing, detecting, responding to, and recovering from agricultural threats. It is difficult to develop a coordinated emergency plan for agriculture because there is no publicly-available, in-depth, interagency or interdepartmental national plan for defense against intentional introductions of biological agents directed at agriculture. While the Animal and Plant Health Inspection Service (APHIS) does have emergency plans for dealing with unintentional introductions of plant and animal pests and pathogens, they are not adequate for responding to agricultural bioterrorism incidents.

Specifically, there is poor industry/government interaction and cooperation. In addition, state-based incident command structures and plans are not well-defined or integrated with industry.

[16] InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the National Infrastructure Protection Center) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

[17] National Research Council of the National Academies, "Counting Agricultural Bio-Terrorism," National Academics Press, Washington, D.C. (2003)

Currently, there are limited public/private partnership capabilities.

Current efforts include a food ISAC which is being restructured toward some of the above goals. APHIS has a reporting system and a National Animal Health Emergency Management Steering Committee (NAHEMS). Other networks do exist even if *ad-hoc* or informally, such as the animal health emergency response system and state veterinarians.

Capabilities for a Uniform Surveillance and Reporting System:

Currently, there is no uniform reporting system for *all* zoonotic diseases but, as identified above, there have been programs and proposals moving towards this capability. The requisite funding to fully implement and create these programs and proposals seems to be stalled. In 2000, the CDC sponsored the West Nile Virus National Surveillance System or ArboNet that now includes all 50 states. Surveillance data is simultaneously collected on humans, horses, mosquitoes, dead birds and sentinel chicken flocks. An offshoot of this is the National Zoo Surveillance System or ZooNet which started in 2001 as a pilot project sponsored by the CDC to include animal data not normally found or integrated into traditional surveillance channels. ZooNet now represents 157 zoos and animal facilities that submit samples for West Nile Virus testing through the Cornell University Animal Health Diagnostic Laboratory. Some additional funding was provided by the Ellison Foundation and put towards the creation of a Web-based system to provide approved parties with automatic updates. ZooNet is distinct because it is the only animal disease surveillance network to share real-time data on disease threat with public health nationally.

A framework for a National Zoonotic Surveillance System has also been proposed. The basic concept is to expand the reporting system to other agents and to bring in additional veterinary diagnostic labs to maintain real-time diagnostics and reporting. The goal is to deploy a nation-wide data network that centrally collects animal health and diagnostic information, and allows access by epidemiologists, public health officials, and defense agencies to real-time analyses and reports. The purpose of such a system is to be able plan responses to a potential epidemic as an early warning system for the infection of humans. Over 2000 participating organizations would give inputs to the system which would include zoos, veterinary clinics, wildlife rehabilitators (both captive and free-ranging). Through routine sampling and medical exams using existing infrastructure within these organizations, it is projected that a new working national system could be operational within a year. Costs are estimated at $1.95 Million for the first year, and $10 Million over 5 years the full implementation and operation of the system.

Basically, the technological and the architectural wherewithal to produce a national surveillance system for zoonotic diseases exists, but has not been harnessed to the task. While coordination of animal and plant entities with public health, law enforcement, and state, local and federal governments and industry was rated as one of the top priorities for federal emphasis, there is still a very long way to go in achieving coordination objectives for all of the operational environments.

State of the Art:

From a technology perspective, all the hardware and software that such systems would require are available today. This includes multi-level security on information system, XML for data tagging and tracking, and ICS technologies.

Technology Limitations and Barriers:

The barriers that need to be overcome, beyond those that are organizational and financial, relate to system scalability, information systems architecture, rural digital signal bandwidth availability, dialogue design/human factors system usability, and reporting format development.

The main thrusts of the work that will be required to realize these coordination goals will be largely concerned with devising appropriate field study tactics, techniques and procedures and integrating this information into an overall crisis

field communications plan. This requires creative development cooperation between discipline specialists and IT professionals during systems development, followed by thorough human factors assessment of system usability. This would be an iterative approach to development of design specifications and adoption of standardized field observation and reporting practices.

Design issues include compensating for lacking ontology/terminology or standards for communicating information on genomics and proteomics. Also, the architecture must accommodate requirements for standardized reporting at all levels and across all involved disciplines, which does not yet exist.

System portability, reliability, and usability across the various operational environments are a significant issue, especially where work has to be done in environmentally challenging settings.

It will be important to involve the diagnostic laboratories in the design process for helping determine approaches to field and follow-on diagnostics, test result interpretations, reporting systems, and reporting formats.

Finally, the coordination needs in the MRPA area share most technical characteristics and many users with the general and specialized coordination needs addressed under other NTROs. Moving forward with special purpose networking systems in any of these areas could erect new barriers to effective collaboration and coordination during planning and response phases.

Gap Fillers:

The major goals can be roughly broken down into two general areas: (1) issues concerning networking in an organizational sense; and (2) issues concerning networking from a data integration and technical communications sense. The organizational issues include such concerns as industry incentives for cooperation, pre-trained teams for responding to outbreaks and better integrated command systems. The data integration and technical communications issues include development of trace-back data systems, hotline services, and common communications across operational environments, uniformity and standardization of data requirements, and linking mechanisms among technically relevant networks (networking across networks).

The strategy for approaching these networking and coordination problems that seems most attractive at present is one of building on the ongoing efforts of those organizations that have already demonstrated initiatives and operationally sound networking systems for which demand can be demonstrated. These various initiatives can be nourished and expanded through helping provide expansions of capabilities and a sound annual funding base for their continued operation. Private sector industries that remain unmotivated to cooperate with the federal biodefense program at DHS and elsewhere can be dealt with in a regulatory fashion. This would be an overall "carrots and sticks" approach that can be selectively applied where it is important to national security to do so.

In all cases these efforts should be conducted in coordination with efforts to increase coordination capability needed for other NTROs.

MRPA.3 – Identification of Outbreak Origins and Spread. *The ability to track movements of animal and plant shipments and plant pest outbreaks and to identify the origin of individual animals and the spread of pestilence.*

Goals:

- GIS enabled systems.
- National secure database.
- DIDA capabilities applied to tracing.
- All possible movements of infectious animals must be identified as quickly as possible and modes of potential spread eliminated.
- National identification system is needed for livestock.
- Expansion of diagnostic network worldwide to track multiple pest outbreaks.

- Trained and equipped staff in shipment tracing and evaluations.
- Trained staff are needed for overt and covert monitoring of international and domestic movements of infectious substances and pests, including training in pattern recognition and analysis, offshore staffing and surveillance capabilities.
- Ability to trace and track processed crops and livestock optimally down to the individual animal level.
- Access to an integrated tracking system that includes purchasing, identification, sale and distribution records.
- Ongoing global risk assessment and pathway analysis.

Current Capabilities:

The National Research Council has stated that information about agricultural diseases and infestations in foreign countries is often vague and not always time-sensitive. Since substantial expertise in exotic plant, animal, and insect diseases does exist in other countries sharing information, ideas, and programs through international scientific collaboration would be able to help fortify our national system for safeguarding plants and animals against intentional threats.

Regarding plants, even a serious plant disease in a populated area can go undetected for a very long time, and as such, domestic surveillance needs to be bolstered. Infrared remote sensing technology for crop analysis exists but is not generally applied to disease propagation.

Work is being done on animal tags and information systems to determine the history of diseased animals and to allow rapid intervention to limit an outbreak. The FDA has recently published draft regulations for trace-back information reporting for the agriculture industry for public review and comment. In addition, the European Union has recently completed a large study on different methods for storing animal history information in or on the animal. Different methods were found to be suitable, including chip-based methods. Being able to pinpoint the movement of a specific animal in relation to its potential contacts and infection is very useful aid in trace-back during an outbreak. This is an area that can be further developed. However, while the technology itself generally exists to support further development of these goals, factors such as limitations on funding availability and political will have restrained progress across all the operational environments.

State of the Art:

Different sources can be useful for identification of outbreak origin and spread information. This includes county extension agents, state veterinarians and departments of agriculture and wildlife, the American Farm Bureau, and APHIS intelligence. For foreign outbreaks, the World Health Organization and Office International des Epizooties (OIE) organizations can be queried through their Internet information services.

Geographical information systems offer promise for such analyses and for sentinel systems deployment. Sandia National Laboratories, for example, has done productive work in this area and has been demonstrating a relevant system offering recently. Some of this work is also being accomplished at state departments of agriculture and wildlife, land grant universities, and at APHIS laboratories.

Technology Limitations and Barriers:

Some of the analytical modeling work has gone beyond the capacity of the current scientific knowledge base to support its further development. This technology is limited, for example, by the fact that many plants have not had their genomic structures established. Pathogen genomics is also far from completely understood. Yet, tracing is somewhat dependent on applications of bioinformatics, and of comparative and functional genomics for understanding specific origins and comparative threats of foreign pathogens.

Gap Fillers:

Identifying origins of specific pathogens and plant life is a valuable analytic tool. Tagging and information systems can assure that the history of a diseased plant or animal in commerce can be traced back to its source to help determine the source of an outbreak; for successful intervention it would also be useful that all plants and animals that have moved through the relevant loci can be rapidly located and sequestered as well. Tracking diseases of wild animals poses different problems; some populations could be tagged and locations monitored but the value and cost of such an approach is unclear at present.

Some specific legal and policy amendments to existing statutes are needed to treat intellectual property rights issues, confidentiality issues, and balance scientific information sharing vs. divulgence of national security-sensitive information. The last issue is equivalent to optimizing access to DNA repositories through properly balancing these two competing areas of consideration.

Two review projects seem particularly relevant to this capability. One would be an interagency cooperative review of remote sensing capabilities for detecting crop disease and contamination. This project would involve the various agencies that do satellite and aerial surveillance of geographical areas (see MRPArto.3 (*Overhead Imaging for Wide-Area Surveillance and Assessment*). The other project would review what remains to be done in developing the chip-based solutions to trace-back for tracking the movements of livestock, harvested plant crops, and food products from origin to the points of retail sale (MRPArto.4 (*Trace-Back Capabilities Using Information Systems and Tags*)). All the indications are that the technology in both cases is ready to place into commercial operations. Issues of costs to producers, processors, and consumers now need to be examined. Cost/benefit of commercialization needs to be analyzed

MRPA.4 – Animal and Plant Diagnostic Surge Capability. *The ability to rapidly mobilize (hire, contract and deploy) private animal health professionals or qualified diagnosticians and other emergency responders (public and private) in a crisis situation.*

Goals:

Animals:

- Sufficient numbers of trained personnel available on two weeks or less notice to assist in an outbreak. There is no firm general estimate on how many persons this might usually involve, but it could range up to several hundreds of thousands for a major national event.
- Ability to identify the numbers of responders: trained personnel and support personnel.
- Mandatory requirements for certification in responding to large-scale animal emergencies for all vets in training.
- Development of nationwide State Animal Response Teams (SART) teams.
- Online capability to approve surge personnel rapidly for foreign animal disease diagnosticians.

Plants:

- Surge capability for qualified diagnosticians to respond effectively to outbreaks and to assess potential outbreaks.
- National and state notification tree.
- Technological advances would curtail outbreaks by expanding the use of digital cameras, electronic communication of pest photos and impacts, and treatment strategies.
- Incentives for private sector/industry to become involved.
- Security clearance issue – more are needed for more existing personnel and surge personnel.
- Draw upon trained global resources.

Current Capabilities:

A number of states have recently just begun to develop mutual assistance agreements with

adjacent cooperative status to realize veterinary and diagnostic surge capability expansions for emergencies. Federal-state cooperation has been better for addressing these objectives in the human health and food/feed environments than for animal and plant agriculture. Leadership and voluntary initiatives in support of this area and others is growing on the part of associations, especially associations such as the American Phytopathological Society and different veterinary medical associations and state diagnostic laboratory associations.

There are a number of organizations or organizational structures that can be used for surge capacity. These include:

- EMAC (Emergency Management Assistance Compact) agreements.
- TEW (Terrorism Early Warning) type virtual surge capacity.
- Veterinary schools and their students in large-scale emergencies.
- Mutual aid agreements among adjacent states.
- VMAT (Veterinary Medical Assistance Teams) can find a helpful place in veterinary and diagnostic surge capacity expansions.
- SART (State Animal Response Teams) also have a place but exist only in a few states.

However, drawing upon human resources across operational environments, the capability is not available for the animal and plant environments but is marginally so for the other areas.

State of the Art:

Building surge capabilities for diagnosticians presents substantial challenges in coordination, training, orientation, and mission management. That capability does not yet exist for the animal and plant communities. It has advanced forward further in the human health, food processing, food distribution, and feedstuffs communities.

Precedents exist, however, such as the emerging network of Terrorism Early Warning (TEW) groups, based on the Los Angeles County TEW model and similar intelligence fusion centers and their technologies. The Medical Response (MR) NTRO discusses telemedicine applications in support of this objective, development of field laboratories and other measures as stop-gaps and surge support.

The National Animal Health Laboratory Network (NAHLN) is a potentially valuable surge capability resource. It is moving toward bringing the APHIS national laboratories and state and university labs together into a networked community, along with CDC's Laboratory Reporting Network (LRN) and FDA's Food Emergency Reporting Network (FERN). Also, it can support training and certification needs and coordinate with the appropriate academic institutions. The National Plant Diagnostic Network (NPDN) is the plant field's analogous entity, but its funding did not survive Congressional review in the last cycle.

Technology Limitations and Barriers:

A limiting consideration in building a surge capability in the U.S. at this time has to do with the fact that government has lost a large amount of its previously available personnel pool in USDA, APHIS, and other relevant federal agencies. States are, therefore, increasingly unwilling to rely on federal personnel resources that might or might not be available or sufficient when needed. Consequently, states especially interested in this issue are increasingly developing their own plans and programs. However, budget limitations of states have restricted relevant personnel to skeletal levels in many of our states. Another problem is that small animal veterinarians have rather different skill sets than large animal veterinarians. The two specialties are not the same and therefore cannot always be tapped into for surge.

These personnel and budget limitations place a heavy responsibility on technology to compensate for them. There are the problems of maintaining human resources databases and of developing communications and coordination mechanisms for contacting and using them productively. Outbreaks require the swiftest possible

interventions for containment and mitigation. However, the necessary technologies already exist and could be made quickly available with the necessary financial resources and incentives.

Gap Fillers:

The animal and plant diagnostic surge capability problem could be addressed by:

- Expanding these capabilities through support to the two major agricultural diagnostic associations;
- Creating the proposed center for plant biosecurity at Ft. Detrick;
- Engaging university departments of plant pathology and schools of veterinary medicine through collaboration with the proper associations in organizing conferences on emergency programs for agricultural mitigation and recovery;
- Development of database and communications networking systems for this particular application; and
- Provision of a small number of demonstration grants to support promising initiatives on the part of state departments of agriculture.

None of these have a particularly high technological content. To some extent surge will be facilitated by the decision support technology that will be encouraged via MRPArto.1.

MRPA.5 – Vaccination/Treatment and Protection. *The ability to produce, distribute and administer large numbers of safe and secure vaccine doses, or alternative treatments, for highly contagious animal diseases, and distinguish vaccinated animals; the ability to make crops and livestock more resistant or less susceptible to disease and threat agents.*

Goals:

Animals:

- Limitation of the number of animals that must be sacrificed.
- Restoration of ability to export if "clean" animals can be distinguished from exposed ones.
- Multivalent vaccines needed to be useful at multiple stages of exposure.
- Animal vaccine stockpile to respond to any likely threat.
- Vaccine procedures are needed for free-ranging wildlife.
- Strategic and fieldable stockpile of vaccines and therapeutics; accessible to emergency responders under expert supervision.
- Rapid prioritization of vaccines needed; production of vaccines appropriate to size of incident.
- Marker vaccines (that indicate prior exposure).
- Government sponsored orphan (low production) vaccines.
- Modeling of vaccination strategies (for cost effectiveness, etc.).
- Alternatives to widespread aerial chemical control of insect vectors of human, animal and zoonotic diseases.
- Ability to draw quickly upon the global vaccine stockpile.
- Development of alternative treatment (systemic treatments are very expensive).
- Improved knowledge on host resistance to diseases.
- Maintain broad and diverse genetic base for plants and animals.

Plants:

- Establishment multi-pronged treatment measures including biologicals for dealing with resistant diseases.
- Secure doses (chemicals and biologicals) are needed for treatments, including credibility of

same for efficacy, purity, and safety; ensure swift distribution.

- Better validation of treatment methodologies.
- Improvement of plant genetic resistance through classic breeding techniques, genetically modified organisms (GMOs) and other mechanisms.
- Improved understanding of foreign/exotic plant diseases and pests.
- Assessment/modification of regulations to rapidly approve (1) access to genetic material; and (2) development of new crop lines and their field utilization.

Current Capabilities:

Development and production of vaccines and alternate treatments is a slow moving process, and the capability is hampered by economic and political issues. There is no current capability to make vaccination production and administration decisions from an economic standpoint. Conflicts exist between trade issues and security issues. There is also a gap between publicly funded research and private industry needs. The science exists but costs and commercial considerations raise barriers to company initiatives. There is also insufficient industrial capacity to produce new vaccines quickly; it takes months to ramp up production (domestically). The orphan vaccine issues are not being addressed

State of the Art:

The state of the art in vaccines and alternative treatment/protection is advanced and vaccines are available for numerous diseases and species. A recent announcement has been made that an effective West Nile Virus vaccine is even now available. A number of the new vaccines have been given conditional approvals, which make them available for release, but they lack confirming tests of efficacy. Other vaccines still are considered experimental and can be released only through an emergency declaration.

Current research emphasizes recombinant DNA-based vaccines, virus-carried vaccines, subunit vaccines and study of bacterins. For wildlife uses, emphasis is being placed on oral vaccines available through salt licks, range cubes and other feeding devices. Water and aerosol administration is also being contemplated as alternatives to injection methods.

Other kinds of treatments and protective measures being emphasized at present include crop "hardening" through genetic modification or the use of GMOs, and classical breeding methods for disease resistance. Other treatment development approaches emphasize fungicides and bactericides, and prophylactic sprays. However, while the science for GMOs development as well as commercialization exists, it is currently a very controversial political issue, and remains even more so for Genetically Modified Animals.

The traditional mass euthanasia/mass vaccination strategies are coming increasingly into question, as a result of the European experiences. Vaccination ring strategies are being examined. Quick tests are being emphasized as ways to guide vaccination strategies. Epidemiological models taking weather variables into account are also receiving special attention with respect to vaccination and mass euthanasia. These newer, more discriminate, strategies may place a greater burden on testing and on skilled personnel.

Technology Limitations and Barriers:

The main barriers limiting progress in the vaccines area are not technical, but rather financial and political. Vaccines development is very costly. When there is an insufficient market to induce the private sector to assume these costs, government can be given a heavy cost burden. Animals and plants have not been given the political or financial support that the human vaccines have received. This seems unlikely to change unless what is perceived as a low probability threat becomes a reality. Plant vaccination[18] program cost-benefit estimations are more marginal

[18] Technique is similar to human/animal vaccine; involves inserting small amount of DNA from virus into plant's chromosome allowing the plant to recognize and destroy a virus when it attacks. It gives the plant the ability to see what the virus looks like so that its defenses are ready. Unlike traditional vaccines, however, immunity from a plant vaccine passes onto succeeding generations.

than those calculated for livestock vaccines. The neglect of insect vectors still remains, but that situation may improve because of the West Nile Virus experience and an effective vaccine for the disease. Delivery methods for vaccine administration of vaccines to livestock and wildlife represent a difficult challenge that is not present in human vaccination situations.

The most limiting factor in new vaccine development from a technological and scientific perspective relates to the lack of fundamental knowledge of genome structure, and the molecular biology of disease processes and associated pathogens. This, however, is just a negative way of saying that the most promising prospect for advancing vaccine development depends upon making major investments in animal and plant genomics.

Gap Fillers:

There are three major areas of special technological emphasis that can be identified to aid the process:

- Applied research on developing new multivalent vaccines, marker vaccines, and orphan vaccines;
- Inexpensive but accurate field screening tests for quickly discriminating between healthy and infected animals (for guidance of containment efforts through vaccination); and
- A vaccine production program capable of meeting large crisis needs for selected diseases.

The USDA, in cooperation with DHS and other entities, has recently completed a draft report on a national agricultural vaccination program plan. Currently, the report is not publicly releasable.

It is clear that the main needs are in the areas of development and production of vaccines and other treatments rather than innovations in responder distribution and administration of these treatments and prophylactic measures. Therefore there is little in this functional capability of immediate interest to technical development as Project Responder is now defined.

MRPA.6 – Quarantine, Isolation and Recall.

The ability for responding agencies (to include industry) to segregate, condemn, detain, or recall contaminated plant/animal/food/feed.

Goals:

- Expansion of offshore data collection for determining potential pests that can reach U.S. shores.
- Determination and prioritization of lists on pests.
- Extensive domestic and international "data mining" to seek information on control strategies.
- Ability to safely and rapidly secure, isolate, and transport suspected infectious or contaminated material for evaluation.
- Ability to rapidly quarantine infected, infested, or exposed areas, plants, animals, or commodities and to initiate delimiting surveys.
- Threat Analysis Critical Control Points program schema and execution plans to combat deliberate disease/adulterants, contamination of raw materials, and processed foods (similar to the Hazard Analysis Critical Control Points programs used to combat natural risks).
- Ability to modulate and communicate permeability of quarantine zone (for roads, ports, airports, etc.).
- Ability to enforce quarantine zones and critical control points.
- Biosecurity of quarantine facilities needs improvement where they exist.
- Establishment of perimeters or perimeter security for plants, animals. See also R&R.3 (*Establishment of Perimeters*).
- Legal authorities to enforce quarantine.
- All goals apply to protective isolation as well.

- Quarantine facilities – improve biosecurity (*e.g.,* mosquitoes).
- National real-time permitting system.
- Ability to access database from MRPA.1 (*Rapid Diagnostics and Detection*) at all quarantine systems.
- National ID system for plants/animals.
- Reduction of quarantine time; varies by species/agent.
- Unaffected animals in quarantine zones need to be fed and cared for.
- Ability to shut down air corridors.

Current Capabilities:

Quarantine and containment facilities exist at present. There are three national facilities and additional facilities located at airports and in private facilities. USDA and FDA have well established and workable systems for food recall.

More research is needed to develop and test epidemiological models for plant and animal pests and pathogens so that optimal eradication and containment strategies can be developed before a threat agent is introduced.

Eradication plans that have been tested, ideally in the area of origin of the target pest or pathogen, need to be developed. Such complex programs are unlikely to be initiated and accomplished in a timely fashion if plans are made on an *ad hoc* basis.

Capabilities for human health are not applicable in this context because humans are not quarantined for exposure to contaminated animals, plants, food, or feed. See PHRBAE.5 (*Isolation and Quarantine*). However, humans can carry diseases affecting animals such as West Nile Virus.

State of the Art:

The basic technology exists for targeting animals/plants/foods for isolation, areas to quarantine, and for rapid food products recall. Accuracy and reliability might be enhanced further, however, through recourse to military predictive modeling software and other associated technology. General availability of these technologies is marginal in the near-term, however, because of costs limitations, knowledge limitations, and modeling content. Therefore, there is every reasons to expect that a large-scale, multifocal outbreak would quickly overwhelm resources as mentioned above.

Gap Fillers:

Three RTOs were developed to improve upon the present state of the art in this area. MRPArto.5 aims to develop a *Threat Analysis Critical Control Points Program* to help protect the food chain; MRPArto.3 (*Overhead Imaging for Wide-Area Surveillance and Assessment*) addresses overhead surveillance capabilities for detecting and isolating geographic areas affected by outbreaks; and MRPArto.6 (*Modeling of Plant and Animal Outbreaks, Surveillance, and Response*) addresses modeling tools to optimize planning for and responses to outbreaks.

MRPA.7 – Rapid and Humane Euthanasia and Disposal of Contaminated Carcasses, Plants and Food Products.

The ability to humanely kill and dispose of up to thousands/millions of animals and plants within 24 hours of detection of disease or exposure and to destroy plant pests.

Goals:

- Limiting spread of disease and ceasing production of infectious particles as quickly as possible.
- Assessment of port and regional facility incineration and laboratory autoclaving capabilities.
- Identification of appropriate rendering, slaughter, landfill, cremation, compost, and burial facilities.
- Ability to safety transport contaminated livestock to burial.

- Ability to burn continuously at 2000 degrees (required to destroy prions, CB agents, fats, proteins).
- BSL-3 slaughter facilities.
- Temporary refrigerated storage of carcasses/plant materials until disposal.
- Need a more adequate understanding of the toxic biological products of massive animal disposal.
- Needs for environmentally safe disposal and euthanasia procedures.
- High numbers (poultry houses) and high mass loading (as in elephant/whale disposals) throughput – slaughter and burial.
- Animal welfare needs to be considered.
- Information on costs and impacts of alternative measures (burial, composting, incineration).

Current Capabilities:

Animal carcass digesters exist, but are not widely fielded. These are being modeled to be portable, but this will not solve the scalability problem. In Europe, plasma destruction has been used as well as a dirty transport corridor from contaminated area to burial area.

Current techniques include rendering, incineration (open and curtain), and burial (on-site or in landfill). However, there is limited landfill capability. Mass burial and burning are the main alternatives to disposal of infected and potentially exposed animals. Both are expensive, repugnant to many, and raise environmental concerns.

Although these types of technologies exist for disposal, capabilities vary depending upon incident characteristics. For example, the technology is simply not the same for 800 lb steer as it would be for human bodies. The technology is suitable for dealing with smaller amounts but in a big incident how would we be able to scale up? What process for 1000s works for 10,000s? There are no large scale humane slaughter methods.

A similar concept applies for the capability in food distribution: if there is a problem at one restaurant chain, they have the capability to destroy and dispose of contaminated food: if the problem occurs at many restaurants on a nationwide basis, it becomes more difficult to overcome. While capability exists to deal with biological agents in the food processing environment, if radiological or chemical agents are used, there is not the desired capability. Capabilities vary depending upon type of agent and size of event.

State of the Art:

Euthanasia and disposal technology exists in all the four applicable environments, but is somewhat less suitable and available for animal carcass disposal than for plants or food products. The only facility with BSL-3 biosafety capabilities for work with large animals that also includes measures for worker protection is Plum Island. It could take five years to build a comparable facility at Ft. Detrick. Protective suits for individuals involved in euthanasia and disposal of contaminated carcasses exist, but do not permit active work while wearing them for very long work periods. At present, there is no alternative to the burial/landfill and burial methods that had to be used in England for the FMD cattle disposals. Bio-bag systems for transporting large animals or large numbers of smaller animals can be useful for transport safety purposes. Animals, harvested plants, and food can also be quick-frozen in preparation for safe transportation and subsequent disposal. There is technology also for breaking down and microwaving remains for sanitary disposal purposes.

For humanely euthanizing animals, aerosolized chemical agents deserve consideration.

Technology Limitations and Barriers:

Plant crop disposal presents some special problems that can degrade effectiveness in destroying diseases of concern. One such problem relates to the fact that plant diseases sometimes choose alternative hosts. For example, soybean rust has

kudzu as an additional host. Soybean rust is of particular present concern because of its extreme transmissibility and the fact that it is presently endemic in Mexico. Another example is *Ralstonia solanacearum Race 3, Biovar 2*, which causes Southern Bacterial Wilt. The initial entry into the U.S. was on geraniums found in greenhouses from several states this last winter. However, this pathogen is known to be a pernicious pathogen of potatoes, causing serious losses in Europe in recent years. It will also attack other solanaceous crops such as tomato, pepper, tobacco and some weed species. It survives in soil and in temperate and subtropical climates in soil and host weed species.

Weather and climate effects greatly affect the survivability, wind-borne transmission, and replication ability of crop pathogens. Tropical climates especially are preferred by many pathogens, which is reflected by the abundance of varieties of tropical diseases, many of which still have yet to be studied and understood for the first time. Weather also affects eradication efforts through incineration and other approaches, as well as the geographic spread of incineration byproducts.

The three main limitations of present technology have to do with portability, scalability, and contamination avoidance in carriers. There are no portable disposal systems capable of more than very small-scale disposal problems. Different technologies are needed for large-scale, numerous-animal disposal needs, with no fully satisfactory methods available. Contamination avoidance through transportation carrier and storage container systems is still in need of systematic environmental engineering study and associated new system design.

On animal euthanasia, aerosol applications for mass humane euthanasia require highly skilled operators. Also, aerosol dissemination has other well-known problems when conducted in open environments that can degrade effectiveness and produce unintended adverse consequences of various kinds.

Gap Fillers:

The earlier statement that the three main limitations of present technology include portability, scalability, and contamination avoidance provides a good guide in this case for filling gaps. Three engineering development activities would address these gaps:

- Engineering study of portable systems employing digesters and plasma burners for disposal of contaminated animals in field settings (see MRPArto.9 (*Digesters and Plasma Burners*)).
- Development of a prototype prefabricated crematorium facility that can be rapidly constructed on field sites to undertake disposal or large animals in large numbers (see MRPArto.10 (*Prototype Prefabricated Crematorium Facility*)).
- Design specification study of refrigerated transport carriers suitable for the sanitary transport of animals infected with diseases of special concern to national security (addressed through decontamination rather than specialized transport).

Feedstuffs were not discussed much because feed is usually destroyed if contaminated.

MRPA.8 – Decontamination. *The ability to ameliorate the effects of the pathogen or adulterant with minimal damage to animal/plant/food or the environments, including facilities and equipment.*

Goals:

- Quick, effective, and inexpensive post-exposure treatment and prophylactic countermeasures for those responders that are potentially exposed to agents/pathogens.
- Need for further technological development and research on irradiation of food and fiber.
- Rapid tests for efficacy of decontamination.
- Establishment of on-the-shelf work plans for likely pests.

- Discovery of potential "self-imposed" regulatory obstacles (permit requirements, pesticide registrations, etc.) to rapid reaction and to development of needed protocols, plans and agreements for effective response.
- Easier compliance with environmental and legal rules.
- Better fumigation procedures (time and cost) of plant/plant products to make rapidly acceptable for commerce.
- Full decontamination of transportation carriers/facilities that contained diseased animals or plants.
- Metric for decontamination or destruction: maintain commercial viability (or safety in the case of household pets or items of substantial intrinsic value, etc.).
- Utilization of modeling tools for decision support to determine physical boundaries for decontamination (see Chapter VIII (PHRBAE)).
- Faster process than sentinel animals for verifying decontamination efficacy.

Current Capabilities:

Contaminated animals and plants are usually destroyed rather than decontaminated, so capabilities are not always used.

There are approved lists for animal decontamination that contain detailed instructions, but this can be difficult and time consuming. There are limited plume/pathogen/containment models to aid in decontamination planning.

Food processing becomes a liability issue, it is simply easier to destroy it; in addition, there are business incentives to support rapid decontamination of a processing plant or distribution facility. Feedstuffs are usually destroyed rather than decontaminated, so there are no capability concerns for decontaminating feedstuff.

More efficient and effective methods for large-scale sterilization of soils, equipment, and facilities are needed (in the aftermath of euthanasia and disposal).

State of the Art:

Most decontamination approaches involve finding or assessing contamination, applying chemical agents to wash off and kill harmful bacteria or viral agents or toxins and chemicals. Some decontamination procedures, however, use irradiation to sterilize surfaces, food products, etc. Food may be decontaminated by applications of hydrogen peroxide or ozone under some circumstances. Surfaces may be decontaminated using paraformaldehyde or formaldehyde in some settings, but they present a potential HAZMAT problem in disposing of the residuals. Medical or veterinary treatments may be used to treat skin damage or disease resulting from contamination, but that is not directly relevant to this functional capability.

Relevant military research and development activities are in current progress at Edgewood Arsenal and at Ft. Detrick on advanced methods for decontamination.

A key final step is to provide assurance that decontamination has been successful. This can be achieved either by detection technology similar to that which may have located the contamination in the first place, or by knowledge of decontamination effectiveness gained either from first principles or empirical studies.

More extensive discussions of both the decontamination and the sensor states of the art can be found in the DIDA, PHRBAE, MR, R&R and PPE NTROs.

Technology Limitations and Barriers:

The major limitations and barriers in this MRPA relate to food-borne bacteria. Since such contamination occurs routinely and under natural conditions, terrorist recourse to introducing such contamination does not usually become apparent until much later after many individuals become sick. It would be very difficult to discriminate between a naturally occurring gastrointestinal

pathogen and one caused by a deliberate introduction into the food supply.

Higgins *et al.* (1999)[19] concluded that there is utility in rapid detection assays for: (1) prophylactic monitoring of food or water suspected of being the target of a bioterrorist attack and (2) serving as "first use" diagnostics when an otherwise routine outbreak of gastrointestinal illness shows evidence of being something else entirely. The same investigators suggested that the rapid sample preparation techniques and real-time diagnostic assays developed at USAMRIID would allow authorities to perform the quickest and most accurate tests to determine if the threat is real and decontamination or disposal actions are needed.

A number of passenger cruise liners have been plagued by recurrent gastrointestinal pathogens. Part of the problem of decontaminating these ships is attributable to the rough surfaces and many nooks and crannies built into these vessels.

Exotic Newcastle Disease is one good example of the difficulty an infectious animal disease can present in decontamination. It can be carried by humans on nasal surfaces, clothing, shoes or boots, or even on cleaning and transportation equipment. A poultry production facility can only be decontaminated through total destruction or through draconian measures including destroying all the poultry and eggs and removing earth surfaces down to 3-4 feet below the surface.

There is a further problem in recognizing biological pathogens that have been carried into the country in humans, live animals, in feed, or in other ways. Parasites are the most common problem associated with foreign travelers, and they remain poorly treated if at all upon arrival.

Gap Fillers:

Chemical decontamination technology seems to be generally available and receiving appropriate current emphasis by military laboratories. Also, food processing and retail chain restaurants seem generally prepared to engage in appropriate decontamination procedures when needed under ordinary circumstances. However, other public facilities and transport systems such as postage facilities and both cargo and passenger ships still present difficult and time-consuming challenges in decontamination. Therefore, it is suggested that new RDT&E be undertaken to explore new and refined decontamination techniques. The main thrust would involve exploring different forms of irradiation and chemical fumigation to identify potential faster and cheaper solutions to treating especially difficult facilities for decontamination purposes.

Also, a requirement continues to exist for using appropriate low-level and benign irradiation techniques to prevent contamination of foods and to restore food safety when environmental conditions may have allowed bacterial contamination of food or feed to exceed threshold levels or for treatments for reducing pest problems. The USDA has recently approved the use of irradiation for extending shelf life of packaged foods, but this approval has not as yet had much influence on commercial practices.

Two RTOs are suggested for addressing these needs. MRPArto.7 (*Improved Irradiation Methods*) addresses irradiation methods for controlling bacterial, funga, and pest infestations in packages, containers, or large storage and transport facilities; and MRPArto.8 (*Enhanced Fumigation Technology*) addresses fumigation technology for decontaminating food processing and storage facilities, and transportation carriers.

Mitigation and Restoration for Plant and Animal Resources Response Technology Objectives (MRPArto)

MRPArto.1 – Plant and Animal Responders' Decision Aid

Objectives:

A CBR event may well involve exotic damage mechanisms outside of the experience of typical plant and animal professionals, not to mention public safety officers. In surge situations

[19] Frazier, T. W. and D. C. Richardson (Editors), "Food and Agricultural Security," *Annals of the New York Academy of Sciences*, vol. 894 (1999).

relatively untrained people will be called on to perform field assessment roles. This RTO will provide content that will allow plant and animal responders to apply codified knowledge and to reach back to specialists so that they will act to most efficiently assess and identify damage, limit onward contamination, and embark on the correct mitigation strategy.

Payoffs:

Early accurate assessment and initiation of appropriate mitigation is likely to localize the impact and minimize damage. Codification of best practices and making them available in the field will also enable meaningful surge by relatively unspecialized individuals. Wide availability of the systems and content would enable effective surge.

Challenges:

While no unique systems technologies need be developed for this purpose, the wide range of environments in which the system would be used and the need for relatively low cost (especially for use in surge) requires careful attention to system design. Multiple connectivity modes for reach-back would be required. The need for high-fidelity visual component (with a high-end variant involving two-way communication of images) will need to be traded off against cost. If possible, this capability should have an option for implementation as a software add-on to existing responder systems rather than as a stand-alone addition. This RTO should be carried forward in coordination with similar RTOs in DIDA and MR.

Milestones/Metrics:

FY2004: Initial system requirements definition and characterization of cognate available systems; initiation of content development through appropriate contracting means.

FY2005: Demonstration of alternative system concepts using COTS systems.

FY2006: Availability of initial suite of validated content; finalization of commercialization/deployment strategy.

FY2007-2009: Demonstration of improved systems concepts integrating COTS technologies and initial content.

FY2010: Demonstration of final system variants.

MRPArto.1 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	2010	Totals
Plant and Animal Decision Aid	$2.5	$7	$6	$6	$4	$3	$3	**$31.5**

MRPArto.2 – Field Screening and Assessment Tests.

Development of rapid screening tests for animal and plant viral pathogens in conjunction with improved surveillance and trace-back systems offers a way to allow the adoption of new strategies for identification, location, and eradication of diseased animals and crops. It could also help direct emergency responders in employing effective small-scale vaccination strategies.

Objectives:

Build on the research from the Strategic Research Area (see Chapter I) on SBR exposure and elsewhere to develop a cost-effective set of rapid screening tests for plant and animal disease and the presence of CBR agents in plant and animals. These tests should allow identification of the pathogen (ideally including ones not expected in advance).

Payoffs:

Validated screening tests would allow emergency responders simple and inexpensive ways to contribute to initial epidemiological analyses for estimating scope, locations, and rates at which pathogens are spreading across a geographical area. This information can be useful for determining specific containment, isolation, and eradication strategies, including vaccination strategies. This can help limit the number of animals that must be sacrificed and delimit areas that must be sprayed using aerial chemicals.

Challenges:

As a strategically important foundation of sectoral defense, this line of research needs continued emphasis and funding for the entire period of the present planning horizon and beyond. Teaching emergency responders to use, interpret, and report upon these tests is a slowly moving process. Widespread distribution of such tests can be costly.

Milestones/Metrics:

An annual allocation of $30 million seems reasonable if it includes development costs and costs of production and distribution of test materials.

MRPArto.2 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	2010	Totals
Field Screening and Assessment Tests	$30	$30	$30	$30	$30	$30	$30	**$210**

MRPArto.3 – Overhead Imaging for Wide-Area Surveillance and Assessment

Objectives:

Exploit existing imaging technology involving earth orbit satellite and unmanned surveillance aircraft to remotely survey agricultural terrain for the presence of crop plant disease, down livestock, and wildlife remains.

Payoffs:

Different agencies employ this technology for other purposes and the proposed application goes all the way back to the 1960s. Since agriculture covers such a large portion of the countryside, aerospace and aerial sensing technologies could provide a very cost-effective approach to surveillance and detection of emerging or near-term biological impacts of terrorist attacks.

Challenges:

Different agencies have this technology in place and working, but have as yet to develop a cooperative approach for crisis and consequences action and epidemiological intelligence studies. These agencies include NASA, NOAA, and military image mapping and surveillance agencies. However, these uses for platforms such as Predator and military satellite programs require funded missions and approvals from the military/intelligence communities. These programs require substantial budgets in view of the costs of unmanned satellites and unmanned military aircraft operations. High-level approvals would then be needed to permit the suggested uses of this equipment and other program resources.

Milestones/Metrics:

FY2004: Develop an interagency working (steering) group to develop and justify this program in detail and associated applications, resulting in an official authority to proceed.

FY2005: Develop a program for validation and testing representative applications of the technology for food and agriculture surveillance and analysis: conduct several pilot studies of simulated attacks, as scientific payloads on other programmed missions. Obtain approval to proceed into building an operational capability.

FY2006-2007: Create a fully operational mission capability that can become a part of the national's homeland security emergency response armamentarium and test on convenient natural disasters and crises experienced during this time.

MRPArto.3 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Overhead Imaging	$0.4	$4	$25	$25	**$54.4**

MRPArto.4 – Trace-Back Capabilities Using Information Systems and Tags

Objectives:

Validate an optimized system approach to using miniaturized chip technology for tracking plant, animals and food products back to points-of-origin with data updating at critical control points. Review European findings on tagging systems and FDA regulations on data item requirements for these purposes. Undertake field tests of alternative system configurations. Undertake cost analyses of costs for national and international implementation of the recommended tagging and trace-back system.

Payoffs:

This technology exists now and can offer early returns in a health and food safety area of established importance. Implementation of this program will satisfy long-standing calls for developing a viable tagging and trace-back system for use in the different operational environments under current consideration. The system findings will facilitate epidemiological investigations of animal and plant disease outbreaks and help refine and reduce the costs of recalls and destruction of contaminated food products.

Challenges:

FDA has taken the lead on forming data item requirements for producers, but has left the decisions on how to comply in satisfying these requirements to producers, processors, etc. The European studies have shown that a variety of methods for on-animal or in-animal data capture and storage are completely feasible The major challenge will be the overall aggregated costs of operating such a massive information system and the associated investigation and enforcement activities needed to ensure compliance with requirements. The costs will ultimately be paid for by consumers, but they are very high. This RTO should be conducted in coordination with work in the Logistics Support (LS) area addressing tracking and tagging issues.

Milestones/Metrics:

FY2004: Review the appropriate literature and develop a research strategy under FDA auspices to demonstrate a cost-effective system compatible with FDA proposed requirements. Secure the cooperation of the relevant industries to pursue a large-scale validation study.

FY2005: Develop and demonstrate one or more prototype hardware/software system configurations for tests and evaluation purposes.

FY2006: Conduct a series of pilot studies in the relevant operational environments and modify the system as indicated to be necessary.

FY2007: Design and conduct a one-year validation and cost-benefit field study to confirm the efficacy and payoff potential of the system; also, locate interested vendors and solicit bids on system fabrication and purchase costs.

MRPArto.4 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Trace-back Capabilities	$0.5	$4	$4	$5	**$13.5**

MRPArto.5 – Threat Analysis Critical Control Points Program for the Food Chain

Terrorist attacks, like the accidental spread of pathogens and accidental contaminations, can occur at many vulnerable points in the food production, processing and distribution process from the farm to the table. Consequently, surveillance should be exercised at key points in the process to achieve the earliest possible detection of accidental or intentional introduction of pathogens or contaminants. A Threat Analysis Critical Control Points Program modeled after the USDA Hazard Analysis Critical Control Points Program offers good prospects for this kind of target-hardening. This approach, linked with trace-back data systems, could become an important detection and analysis tool for field use.

Objectives:

Use systems analysis to identify the key points in the food chain at which detection is to be attempted and the detection techniques and technologies (including visual inspection) that would be most cost effective. Evaluate alternative concepts of operation for use of these detection technologies (including those developed under MRPArto.2).

Payoffs:

For a relatively modest federal investment, the demonstrated value of the HACCP program devised by the USDA Food Safety and Inspection Service (FSIS) could be extended to underline and enhance industry's cooperation with federal national biosecurity program. Such enhanced cooperation would be a very valuable objective, since such cooperation might be generalized to other aspects of homeland security requiring

voluntary industry cooperation. The program could, at the same time, provide opportunities for monitoring industry compliance with FDA regulations concerning trace-back records compliance.

Challenges:

The greatest technical challenge is the need to determine the most cost-effective detection strategy given the wide range of possible terrorist attacks on the food chain and changing modes of detection that may become available over the next decade.

Milestones/Metrics:

FY2004: Organize a cooperative FDA/USDA task force from the appropriate internal entities to devise a TACCP program plan and draft associated prospective regulations. Invite industry and general public inputs and hold regional hearings with groups from the different operational environments to be involved.

FY2005: Devise and undertake pilot study exercises to confirm that the proposed system will work efficiently and that it is minimally intrusive to business operations. Undertake user surveys of the system to test acceptability.

FY2006: Conduct red team field tests exercises to test the systems usability during a prospective crisis and operator conformity with regulations.

FY2006-2010: Evaluate advanced technology screening systems and incorporate them into the system plan.

MRPArto.5 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	2009	2010	Totals
Critical Control Points Program	$2	$3	$6	$1	$7	$2	$5	**$26**

MRPArto.6 – Modeling of Plant and Animal Outbreaks, Surveillance, and Response

Objectives:

Develop modeling tools for use by cognizant agencies and incident commanders that can aid in optimizing plant and animal surveillance and response strategies.

Payoffs:

Extensions and new applications of this technology can significantly help prevent and mitigate the impacts of foreign pest introductions and outbreaks that threaten agricultural productivity and ecosystems, including plant crops, exotic species, companion animals, livestock and animal wildlife. These measures will enhance human health assurance and national security, as well as protect U.S. agriculture from diseases and contaminations that would jeopardize food and fiber sales abroad.

Challenges:

The U.S. still has deficiencies in its emergency response infrastructures and little experience in coping effectively with large-scale, multifocal terrorist attacks or naturalistic spread of animal and plant disease. The most challenging experience in recent times has been the Exotic Newcastle Disease (END) poultry outbreak which began this year in California. Lack of advance preparation, limited analytic tools and staff limitations thwarted its early control. A post eradication surveillance program is ongoing and a national program for END is tying together education and strategy and working on issues such as how to deal with non-traditional agricultural entities such as live bird markets and exotics in the surveillance chain. It is hoped that this program will eventually include other avian diseases. The proposed technology development effort can address these deficiencies in preparedness to face threats to our agriculture and environment both with respect to ongoing surveillance, analysis, and prescriptive action when a significant crisis is discovered that is amenable to study by remote imaging technology or by epidemiological reporting by producers. One other associated challenge is that of helping discriminate between a natural disease occurrence and an intentional introduction of a contaminant or pathogen through the application of this technology.

Milestones/Metrics:

FY2004: Develop an organizing committee comprised of representatives from APHIS, the DHS

S&T directorate, HHS, Department of the Army, state departments of Agriculture and Wildlife, DARPA, and potentially the Department of Commerce to flesh out a multi-faceted program for surveillance and modeling technology applications to epidemiological analysis, population control, and mitigation actions. Develop an RFP and associated statements of work for use in applications for grant support by university centers, and associated in-house participation by APHIS and other appropriate government research activities.

FY2005: Approve and initiate individual projects in the relevant application areas (animal, plant crops, wildlife, and environmental health).

FY2006: Create an integrated action plan for real-world application of the technology and launch a training program for creating and expanding expertise in selected state university settings, based upon competitive bids.

FY2007: Undertake case studies as outbreak or large-scale contamination incidents opportunities are presented for further assessments of cost-benefit.

MRPArto.6 – Budget in Millions

Thrust	2004	2005	2006	2007	2008	Totals
Modeling of Outbreaks, Surveillance, and Response	$2	$10	$20	$10	$10	**$52**

MRPArto.7 – Improved Irradiation Methods

Objectives:

Find quick, effective and inexpensive prophylactic and post-exposure treatment countermeasures for contaminations and infestations in food and feed through different forms of irradiation.

Payoffs:

Food losses due to bacterial contamination and associated disposal are massive every year, even in the U.S. Developing more effective sanitary methods for preserving food safety would reduce these losses and reduce the associated food-borne illnesses that attack millions of Americans every year and precipitate associated hospitalizations and mortalities. Fresh fruit and vegetables losses through spoilage would be very significantly reduced. Container facilities and food processing facilities can be made more sanitary, thus contributing to reducing food contamination. Microwave and ionizing radiation represent the two major approaches to food irradiation that have proven helpful thus far.

Challenges:

This technology needs further exploration and refinement. The public has to become convinced of the efficacy of irradiation as a safe means for decontamination. To create a market for irradiated foods, industry needs to be convinced that markets exist for long shelf-life packaged foods treated in this way and that legal liabilities will not threaten the adoption of these food preservation methods. Applicator personnel safety can be a particular health problem and legal liability if accidents occur in the commercial use of this technology. Little is known yet about the biological effects of EMP beams, which are used mostly for military purposes at this time. The human health hazards of exposure to lasers, microwaves, and ionizing radiation, of course, can be substantial.

Milestones/Metrics:

FY2004: Undertake a literature review and then design an experimental R&D program for extending the state of the art in this application area in different operational environments and task appropriate national laboratories to design the different individual project tasks involved.

FY2005: Integrate the individual studies into an overall program proposal and commence pilot studies work following an authority to proceed by the DHS.

FY2006: Specify the replanning suggested by initial pilot study findings and begin a one-year formal study effort.

FY2007: Analyze results and develop demonstrations and orientation materials concerning

commercialization of the validated technology for industry and government.

MRPArto.7 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Improved Irradiation Methods	$3	$3	$10	$5	**$21**

MRPArto.8 – Enhanced Fumigation Technology

Objectives:

Fumigation technology has been used for a long time and military chemical commands know a lot about how to use it effectively. Nonetheless, the recent experiences in decontaminating congressional buildings and postal facilities following anthrax mailings to these locations vividly illustrated the complexities and major outlays needed in manpower time and costs that the current state-of-the-art technology requires. An associated objective is to find cheaper and more efficient ways to decontaminate transportation carriers such as cruise ships, ambulances, food storage facilities, and food processing facilities.

A variety of contaminants and biological pathogens are of concern here, such as parasites, pests, molds, spores, bacteria and viruses. So this review would be concerned with: (a) contaminants and pathogens (including toxins), (b) different decontamination agents, and (c) facilities and containers (large and small).

Payoffs:

The resulting recommendations from this extended study activity could be used as the basis for undertaking a major DHS initiative in improving new contamination technology utilization. The longer-term payoffs include improved food safety, positive impacts on animal and human health, and reduced losses in agricultural and food products domestic sales and exports due to contamination and spoilage.

Challenges:

The main procedural challenge to this study project is that some of the most relevant information is classified by military authorities. The findings would need to be edited so that they do not convey useful information to potential terrorist adversaries. This is a rather routine challenge that is faced frequently when dealing with sensitive matters that affect national security. The other main consideration is that of ensuring that the study panel that is organized and the outside contributors brought into meetings to make additional technical and scientific contributions are carefully chosen.

Milestones/Metrics:

A two-year study effort is envisaged: (a) a first year effort concerned with study design and topic selection, as well as panel organization and identification of desirable outside contributors; and (b) a second year concerned with the conduct of review meetings and preparation of the committee report.

FY2004: Perform the detailed review study design and develop the needed expert human resources.

FY2005: Undertake the actual study program and publish and distribute a final report including recommendations.

MRPArto.8 – Budget in Millions

Thrust	2004	2005	Totals
Enhanced Fumigation Technology	$1	$2.5	**$3.5**

MRPArto.9 – Digesters and Plasma Burners

Objectives:

Undertake a literature review on portable systems for carcass disposal and develop a program for ascertaining the relative strengths and weaknesses of the individual systems and their operational capacities, limitations, and costs of procurement and operation in representative field settings.

Payoffs:

These systems exist and have been used in Europe. We have not yet found technical literature that describes the strengths and limitations of these systems sufficiently or whether they are available from U.S. suppliers. Nonetheless, some pathogens such as BSE and its human counter-

part require extreme heat for their destruction. Also, in cases of large masses of carcass materials disposal, minimal ash residuals or other residuals can be significant attractions.

Challenges:

The main technical challenge has to do with determining how far these technologies can be taken for large-number and small/medium-animal disposal situations.

Milestones/Metrics:

FY2004: Undertake an engineering study as described above.

FY2005-2007: If findings show continued promise, procure several units and test their operational capacities, limitations, and costs of operation in field settings.

MRPArto.9 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Digesters and Plasma Burners	$0.5	$1	$1	$0.5	**$3**

MRPArto.10 – Prototype Prefabricated Crematorium Facility

Objective:

An important part of preparing the nation to become capable of managing large-scale agroterrorism incidents is to develop a better way to dispose of contaminated carcasses and plants. It is neither practical nor economical to build crematorium facilities for burning carcasses and contaminated harvested crop materials all over the country. However, a prefabricated system that could be erected and made operational in a matter of several days to alternative sites by trained workers is feasible and could meeting this particular need if and when it arises.

Payoffs:

Availability of this system would be valuable in orienting state governments and emergency responders in agriculture about animal disposal problems. A training facility housing this equipment would allow specific training on the system to be used for emergency responders from cooperating jurisdictions.

Challenges:

The effectiveness of this approach would be dependent upon the number of such facilities available and their distance from the locations from which infected animals or contaminated crops originated. The system would need designed in conjunction with a safe and secure transportation carrier system for deliveries of carcasses and plant material. If multiple focal sites were involved within a particular geographic area served, computer decision support systems involving optimization algorithms would best be used to minimize carrier travel distance and time and optimize avoiding travel through populated areas and travel over heavily used roads during periods of heavy traffic.

Milestones/Metrics:

FY2004: Design and conduct of an engineering study of the general approach.

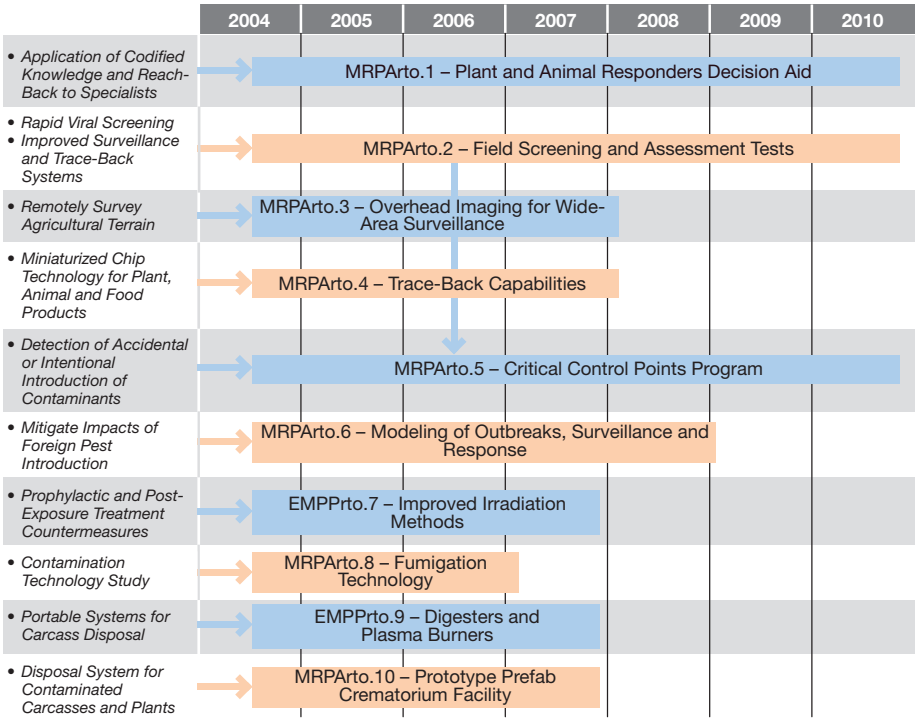
FY2005: Construction of a central facility for design verification and training.

FY2006: Construction and modification of a prototype transportable facility and pilot testing of disposal capacities for a simulated large-scale incident.

MRPArto.10 – Budget in Millions

Thrust	2004	2005	2006	2007	Totals
Prototype Crematorium Facility	$2	$20	$30	$40	**$92**

FY2007: Make needed modifications and begin construction of operational models; begin training program; undertake a supervised simulation with a cooperating entity.



Mitigation and Restoration for Plant and Animal Resources Technology Roadmap

Appendix A

Spiral Development and Commercialization of Affordable Advanced Technology Systems

The need for Emergency Responders to be prepared for catastrophic terrorism has been evident to experts for some time. However, it has only begun to attract sustained government attention and resources since September 11th, 2001.

It was to be expected that, in many capability areas, gaps in responder capabilities could be reduced through straightforward, near-term adaptations (or "transfers") of existing commercial and military technologies. The Project Responder planning effort has verified this expectation and suggests that much relevant investment is already being made by the federal government and industry.

For such an intractable problem as catastrophic terrorism, it was also to be expected that areas would be identified where major progress in eliminating capability gaps would require significant technology investment and even basic research—if progress could be made at all. The current effort has verified this expectation as well.

Finally, in many areas, significant improvement in capability can be expected from near-term technology (and non-technological solutions), yet further dramatic improvements can be expected to result from a later generation of technology. In these instances, technology planners and responder organizations must be concerned that pursuit of ultimate performance levels does not unnecessarily inhibit early deployment of significantly improved systems, and also that early deployment of improved systems does not unnecessarily impede the later adoption of further system improvements. Explicit attention to intermediate design points and upgrade paths can both maximize prospects for a smooth, interoperable, transition where that is feasible, and avoid recriminations about misplaced expectations where it is not.

In other words, technology planning to improve capabilities for dealing with potentially catastrophic terrorism cannot be undertaken in a vacuum; instead it must be cognizant of the channels through which technology will actually be integrated into systems and deployed to improve responder capability. Moreover, while the current project focused initially on responder requirements (or "technology-pull"), room must be made in the S&T process for the fruits of "technology-push" as well (for example, the fruits of work in the Strategic Research Areas defined in the Introduction). A full discussion of how this should be accomplished is beyond the scope of the current project. However, this appendix presents some of the concepts should be considered by the Department of Homeland Security in managing a portfolio of science and technology activities aimed at enhancing future responder capabilities.

As noted in the Preface and Introduction, the decentralized and diverse character of responder organizations means that technology adoption by responders is very different from the procurement process that most federal science and technology planners are used to. Whereas a successful federal technology development program usually leads to federal government procurement (indeed, the term "acquisition" was adopted to describe the combination of development and procurement),

in the case of emergency responders the engineering and manufacturing development (EMD) and production will usually be performed by commercial suppliers. However, the heavy role of government organizations at all levels and the strong requirement for standardization and interoperability means that the market is also very different from the typical commercial market for high technology goods.

Responder organizations have very limited procurement budgets and so it would only take a few instances where a deployed system was unexpectedly rendered obsolete by the next generation, to sour responders on the process. Similarly, commercial suppliers to responder organizations have limited product development budgets, and a key role of federal technology programs will be reduce uncertainty about the future marketplace so that suppliers will have the confidence to invest in developing appropriate products. A cooperative process of integrated demonstration and consensus-building will be an important element of the technology transfer process.

Many of the federal officials and organizations now involved in developing technologies for responders have experience in the Department of Defense. DoD has learned from the commercial market place that attempts to leap a generation of technology and meet specified "requirements" through development of an integrated system using new technology in all the subsystems leads to slower progress as well as the risk of total failure.

By contrast, an "open systems" approach that uses defined (but not permanent) architecture and interface specifications to allow competitive development at the subsystems/level allows both earlier deployment of improved capability and more rapid technological evolution beyond that level. DoD officials have come to understand the need for "spiral development" and "evolutionary acquisition" in order to get systems in the field early that take advantage of current technology and then continually refreshing the technology embodied in deployed systems in order to improve capability over time.

In contrast to earlier acquisition concepts, systems can be deployed for operational use before they are fully developed, and they do not have a predefined end state. Early operational use of new capabilities and new operational concepts enabled by new technology has benefits for operational effectiveness and also for the development process. Getting advanced technology in the hands of users early helps refine the true operational value of the technology and thus helps make design tradeoffs; it also increases the constituency for useful innovations and helps extinguish invalid ones.

Of course, this new thinking in DoD brings DoD much closer to the evolutionary approach that is already typical of industry—in which the notion of working more closely with customers (or a lead customer) in developing new products has taken hold. One key process within DoD for this new approach is the "Advanced Concept Technology Demonstration (ACTD)." ACTDs involve the application of advanced technology to a military problem, but the focus is on the military application rather than the development of the technology itself. The focus is not just on the operational test of a new piece of equipment but generally an assessment of a new operational or organizational approach that is made possible by the new technology.

Both a user organization as well as a technology developer are required as co-sponsors before the ACTD can be initiated. An essential element of the ACTD is that there be a small operational leave-behind capability after the demonstration period has ended.

In the DoD acquisition process, the intended next step after a successful ACTD was the initiation of a formal procurement including a full scale engineering and manufacturing development phase. In the responder world, a successful ACTD-like demonstration would instead be followed by the commitment by one or more commercial suppliers to develop products based on the demonstration. This commitment would likely be facilitated by responder involvement in integrated demonstrations and by a national level

identification of the new capability as an appropriate standard.

Thus the Department of Homeland Security should consider replacing the DoD phrase "evolutionary acquisition" with "evolutionary commercialization and deployment." Beyond this change in words, it will be necessary to calibrate the S&T investment process to the realities of the responder adoption process.

In other words, to be successful, a science and technology effort focused on responder capabilities will affect the assessed demand for, as well as the supply of, technology. Vendors need to feel comfortable with the level of commercial risk in selling a product as well as the technical risk in developing it. Testing and standards and harmonized expectations of future technology availability will be as important to success as increments of technical performance.

While the ACTD focuses on new operational applications of relatively mature technology, an older form of technology demonstration – the "Advanced Technology Demonstration" (ATD) – typically focuses on proving the feasibility of the basic technology underlying a novel system. Such ATDs generally involve system-level tests, though component-level demonstrations are also possible. Because of the expense involved in developing a prototype, such demonstrations are only appropriate if there is a high degree of confidence that the demonstration will succeed. A slew of research and engineering activities, including experiments of various types, must generally be undertaken before an ATD is considered.

The difference between an experiment and a demonstration is that an experiment is primarily conducted for the purpose of learning while a demonstration aims at verification (and perhaps improving the "art" that goes into producing the test articles.) In modern engineering practice, the expectation is that the underlying science will generally be understood before an attempt is made to develop a product based on a new discovery.

Open systems architectures are important to allow innovation to occur at many levels. Some of this innovation will be pleasant surprises to federal S&T planners, and the planning process must be flexible enough to accommodate it. But there is still room for a systems engineering approach that assesses the risk at the level of each system component and helps generate an appropriate level of redundancy in technical approach and in scheduling to reduce the overall risk to acceptable levels.

One element of such a risk management approach is the use of Technology Readiness Levels (TRLs). TRLs are a set of nine graded descriptions of stages of technology maturity. They were originated by the National Aeronautics and Space Administration and adapted by the DoD for use in its acquisition system. TRLs are used by program managers to plan the phases of their spiral development programs. As the program manager considers when to insert a new technology into future evolutions of his system, he or she uses TRLs to understand when the technology will have been matured to the point where there is acceptable risk in using that technology. That way, the continuous upgrade of complex systems can move forward without unexpected perturbations to cost and schedule.

Because complex system developments usually involve the integration of various component technologies that may have different technology readiness levels, and because the integration even of mature technologies is not a simple task, NASA personnel have recently developed Integration Readiness Levels (IRLs) that are useful in assessing development risk and appropriate testing approaches from the point of view of the system as a whole.

The TRLs and IRLs are themselves only descriptions of stages of technical maturity (or risk reduction); by themselves they are not a management tool. However, rules of good practice can be developed that address (for example) the minimum TRL that must be attained before a component is considered for inclusion in a particular

system-level test (IRL). However, compared to the Department of Homeland Security, NASA (even with the increased international participation in its missions) is able to comprehend more of the overall system of concern in its own planning and development process; it controls its own procurement, and it still generally develops systems to a particular requirement rather than envisioning a continual increase in capability. So DHS will need to adapt this system for its more difficult environment and its required focus on evolutionary commercialization and deployment.

Descriptions of the TRLs and IRLs, together with clarifying definitions, are provided in the table below and on the next page.

Technology Readiness Level	Description
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.
7. System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Integrated Readiness Level	Description
1. Concept Systems Analyses Completed	Requires definition of how system components operate together to achieve functionality, together with rough performance specifications for components.
2. Detailed System Design Completed	Interfaces and component characteristics are specified and subjected to engineering analysis and simulation.
3. System Mockup or Prototype, Subjected to Simulated Test Environments	Focus is on risk reduction of novel interfaces and identification of unexpected interactions. Well-defined components may be simulated as well as the environment.
4. Prototype/Demonstrator Exercised in Representative Operational Environments	Focus is on system demonstration in operational environments that may not be fully characterized by simulations.
5. Operational System Deployment	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation.

Clarifying Definitions	Description
1. Breadboard	Integrated components that provide a representation of a system/subsystem and which can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.
2. High Fidelity	Addresses form, fit and function. High fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.
3. Low Fidelity	A representative of the component or system that has limited ability to provide anything but first order information about the end product. Low fidelity assessments are used to provide trend analysis.
4. Model	A reduced scale, functional form of a system, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.
5. Operational Environment	Environment that addresses all of the operational requirements and specifications required of the final system to include platform/packaging.
6. Prototype	The first early representation of the system which offers the expected functionality and performance expected of the final implementation. Prototypes will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.
7. Relevant Environment	Testing environment that simulates the key aspects of the operational environment.
8. Simulated Operational Environment	Environment that can simulate all of the operational requirements and specifications required of the final system or a simulated environment that allows for testing of a virtual prototype to determine whether it meets the operational requirements and specifications of the final system.

Appendix A

Acronyms

2G	General Packet Radio Services (GPRS)
3-D	Three Dimensional
3-D GIS	Three Dimensional Geographic Information System
3G	Universal Mobile Telecommunication Service (UMTS)
3PL	3rd Party Logistics
AAVLD	American Association of Veterinary Laboratory Diagnosticians
AC/DC	Alternating Current/Direct Current
ACPLA	Agent-Containing Particles per Liter of Air
ACTD	Advanced Concept Technology Demonstration
ADASHI™	Automated Decision Aid System for Hazardous Incidents
AFCEA	Armed Forces Communications & Electronics Association
AFRL	Air Force Research Laboratory
AIDS	Acquired Immune Deficiency Syndrome
AIS	Automated Information Systems
ALP	Advanced Logistics Program
ANSI	American National Standards Institute
APDS	Autonomous Pathogen Detection System
APHIS	Animal and Plant Health Inspection Service
ARA	Applied Research Associates, Inc.
ARL	Army Research Laboratory
ASCO	Advanced Systems and Concepts Office
ASOCC	Area Secure Operations Command and Control
ASU	All-Source Situational Understanding
ATCC	American Type Culture Collection
ATD	Advanced Technology Demonstration
BAA	Broad Agency Announcement
BioAlirt	Bio-event Advanced Leading Indicator Recognition
Bio-ToF MS	Biological Time-of-Flight Mass Spectrometer
BSL-3/4	Bio-Safety Level-3/4
BMG	Building Model Generator
BSE	Bovine Spongiform Encephalopathy
BSPS-ESI/MS	Biological Sample Prep System – Electrospray Ionization/Mass Spectrometry
BTCM	Bio Threat Consequence Management
BW	Biological Warfare
C^2	Command and Control

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Common Access Cards
CADB	Chemical Agent Detection Badges
CAMEO	Computer Aided Management of Emergency Operations
CapWin	Capital Wireless Integrated Network
CATS	Consequence Assessment Tool Set
CB	Chemical and Biological
CPR	U.S. Customs and Border Patrol
CBR	Chemical, Biological and Radiological
CBRE	Chemical, Biological, Radiological, and Explosive
CBRNE/HE	Chemical, Biological, Radiological, Nuclear, and Explosive/High Explosive
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive/Incendiary
CBW	Chemical Biological Warfare
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control (and Prevention)
CE	Crisis Evaluation and Management
CECOM	Communications Electronics Command (Army)
CFU	Colony Forming Units
CGNS	Carrier Grade Notification System
CI	Criminal Investigation and Attribution
CICC	Community Intelligence Coordination Center
CINC	Commander in Chief
CMIS	Consequence Management Information System
CMI-Services	Consequence Management Interoperability Services
CMT	Citizen Mobilization Teams
CNN	Cable News Network
CNS	Community Notifications System
CO_2	Carbon Dioxide
COA	Course of Action
CoBRA	Chemical Biological Response Aide
CONOPS	Concept of Operations
COP	Common Operating Picture
COTS	Commercial-Off-the-Shelf
CPIE	Command Post Information Environment
CPOF	Command Post of the Future
CRM	Customer Relations Management
CRNE	Chemical Radiological Nuclear Explosive
CRT	Cathode Ray Tube
CTIC	California Anti-Terrorism Information Center
CW	Chemical Warfare
DAE	Disaster Assistance Employee
DARPA	Defense Advanced Research Projects Agency
DATSD	Deputy Assistant to the Secretary of Defense
DCTS	Defense Collaborative Tool Suite
DEA	Drug Enforcement Administration

DERIS	Domestic Emergency Response Information Service
DHS	Department of Homeland Security
DIDA	Detection, Identification, and Assessment
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DMAT	Disaster Medical Assistance Teams
DMORT	Disaster Mortuary Response Team
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DOE	Department of Energy
DoT	Department of Transportation
DREAMS	Disaster Relief and Emergency Medical Service
DSS	Decision Support Systems
D-S3	DARPA Syndromic Surveillance System
DTB	Mycobacterium Tuberculosis Complex Direct Detection Assay
DTRA	Defense Threat Reduction Agency
ECBC	Edgewood Chemical and Biological Center
EDIS	Emergency Digital Information System
ELINT	Electronic Intelligence
ELISA	Enzyme-Linked Immunosorbent Assay
EMAC	Emergency Management Assistance Compact
EMALL	Electronic (Commerce) Mall
EMAN	Emergency Medical Alert Network
EMD	Engineering and Manufacturing Development
EMERRS	Emergency Regional Response System
EMP	Electromagnetic Pulse
EMPP	Emergency Management Preparation and Planning
EMS	Emergency Medical Service(s)
ENCOMPASS	Enhanced Consequence Management Planning and Support system
END	Exotic Newcastle Disease
ENS	Emergency Notification System
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
ESP	Extranet for Security Professionals
ESRI	Environmental Systems Research Institute
ESSENCE II	The Electronic Surveillance System for the Early Notification of Community-based Epidemics
EXML	Expanded eXtensible Markup Language
FACA	Federal Advisory Committee Act
FAST	PHRBAE.2 (Anteon Prog)
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCE	Functional Capability Element
FD	Fire Department
FEMA	Federal Emergency Management Agency

FERN	Food Emergency Reporting Network
FID	Flame Ionization Detector
FIST	Field Inventory Survey Tool
FPD	Flame Photometric Detector
FRED	Facilities Resource Emergency Database
FSIS	Food Safety Inspection Service
FTIR	Fourier Transform Infrared (spectroscopy)
GC	Gas Chromatography
GCSAW	Gas Chromatography Surface Acoustic Wave
GCSS CINC/JTF	Global Combat Support System Commander in Chief/Joint Task Force
GenCon	Genomic Resources Management and Services
GIS	Geographical Information Systems
GMO	Genetically Modified Organism
GOTS	Government Off-the-Shelf
GPR	Ground Penetrating Radar
GPS	Global Positioning System
GPS/GIS	Global Positioning System/Geographical Information System
GRIP	Global Response Incident Planner
GUI	Graphical User Interface
H&AI	Hicks & Associates, Inc.
HACCP	Hazard Analysis and Critical Control Point
HAN	Health Alert Network
HANAA	Handheld Advanced Nucleic Acid Analyzer
HARC	Houston Advanced Research Council
HAZMAT	Hazardous Materials
HE	High Explosive
HEPA	High Efficiency Particulate Air
HERF	High Energy Radio Frequency
HHS	(Department of) Health and Human Services
HHSA	Health and Human Services Agency (San Diego County)
HIPPA	Health Insurance Portability and Accountability Act
HLS/HDC^2	Homeland Security/Homeland Defense Command and Control
HMO	Health Maintenance Organization
HPAC	Hazard Prediction and Assessment Capability
HPM	High Powered Microwave
HRSA	Health Resources and Services Administration
HSARPA	Homeland Security Advanced Research Projects Agency
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, & Air Conditioning
I&W	Indications and Warning
IAB	(Federal) Interagency Board
IC	Incident Commander
ICD-9	International Classification of Diseases (Ninth Edition)
ICE	Immigration and Customs Enforcement
ICIT	Incident Command Information Tool

ICMS	Incident Command Management System
ICS	Incident Command System
ID	Identification
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical & Electronics Engineers
IFC	Intelligence Fusion Center
IMINT	Imagery Intelligence
IMS	Ion Mobility Spectrometry
IPB	Intelligence Preparation of the Battlefield
IPO	Intelligence Preparation for Operations
IR	Infrared
IRL	Integration Readiness Level
IRRIS	Intelligent Roadway and Railway Information System
ISAC	Information Sharing and Analysis Centers
ISN	Institute for Soldier Nanotechnology
ISR	Intelligence Surveillance and Reconnaissance
ISS	Internet Security Systems
IT	Information Technology
ITS	Intelligent Transportation Systems
JBREWS	Joint Biological Remote Early Warning System
JDST	Joint Logistics Decision Support Tools
JIC	Joint Intelligence Center
JISE	Joint Intelligence Support Element
JPG	Graphics file type (developed by the Joint Photographic Experts Group)
JRIES	Joint Regional Information Exchange System
JSIPP	Joint Service Installation Pilot Project
JSLIST	Joint Services Lightweight Integrated Suite Technology
JTF	Joint Task Force
JTRS	Joint Tactical Radio System
JWARN	Joint Warning and Reporting Network
KIPP	Knowledge and Intelligence Program Professionals
LACRCIC	Los Angeles County Regional Criminal Information Center
LAN	Local Area Network
LANL	Los Alamos National Laboratory
LEADERS	Lightweight Epidemiology and Advanced Detection, Emergency Response System
LEO	Law Enforcement Online
LEWG	Law Enforcement Working Group
LIBS	Laser Induced Breakdown Spectroscopy
LIDAR	Light Detection and Ranging
LIS	Logistics Information System
LPOSS	Long Path Optical Sensor System
LRN	Laboratory Reporting Network
LS	Logistics Support
LSTAT	Life Support for Trauma and Transport
M&S	Modeling and Simulation
MAC	Multi-Agency Command

MALDI	Matrix Assisted Laser Desorption Ionization
MASINT	Measurement and Signature Intelligence
MBLM	Multi-Zonal Blowdown Model
MEF	Marine Expeditionary Force
MEVA	Munitions Effectiveness Vulnerability Assessment
MHz	Megahertz
MIDAS-AT	Meteorological Information and Dispersion Assessment System Anti-Terrorism
MIPT	Memorial Institute for the Prevention of Terrorism
MIT	Massachusetts Institute of Technology
MLS	Multilevel Security
MMMWR	Morbidity and Mortality Weekly Report
MOU	Memorandum of Understanding
MPEG	Motion Picture Experts Group
MR	Medical Response
MRPA	Mitigation and Restoration for Plant and Animal Resources
MTMC	Military Traffic Management Command
NAHEMS	National Animal Health Emergency Management Steering Committee
NAHLN	National Animal Health Laboratory Network
NAI	Named Areas of Interest
NARAC	National Atmospheric Release Advisory Center
NASA	National Aeronautics & Space Administration
NATO	North Atlantic Treaty Organization
NBC	Nuclear/Biological/Chemical
NBCR	Nuclear/Biological/Chemical/ Radiological
NBS	National Bureau of Standards
NC	North Carolina
NDPIX	National Drug Pointer Index
NE	Nuclear, Explosive, and Incendiary
NEDSS	National Electronic Disease Surveillance System
NEST	Nuclear Emergency Response Team
NFPA	National Fire Protection Agency
NGA	National Geospatial-Intelligence Agency
NIFCC	National Interagency Fire Command Center
NIJ	National Institute of Justice
NIMS	National Incident Management System
NIOSH	National Institute for Occupational Safety & Health
NIST	National Institute of Standards and Technology
NMIC	National Military Intelligence Center
NOAA	National Oceanic and Atmospheric Administration
NOC	Network Operating Center
NOTAMs	Notice to Airmen
NRC	Nuclear Regulatory Commission
NRE	Nuclear, Radiological, Explosive
NRIC-VI	National Reliability and Interoperability Council (rechartered)

NSHS	National Seed Health System
NSOF	Network Sensors for the Objective Force
NTRO	National Terrorism Response Objective
NVESD	Night Vision and Electronic Sensors Directorate
OASIS	Organization for the Advancement of Structured Information Standards
ODISC4	Office of the Director of Information Systems for Command, Control, Communications & Computers (Army)
OEM	Office of Emergency Management
OES	Office of Emergency Services (California)
OIE	Office International des Epizooties
OIF	Operation Iraqi Freedom
OFDM	Orthogonal Frequency Division Multiplex
OLES	Office of Law Enforcement Standards
OLETS	Oklahoma Law Enforcement Telecommunications System
OPSEC	Operational Security
OSAC	Overseas Security Advisory Council
OSD	Office of the Secretary of Defense
OSHA	Occupational Safety and Health Administration
OSIS	Open Source Information System
OSMLS	Operating Systems Multi-Level Security
OT&E	Operational Test & Evaluation
PCR	Polymerase Chain Reaction
PDA	Personal Digital Assistant
PEAC	Palmtop Emergency Access for Chemicals
PHRBAE	Public Health Readiness for Biological Agent Events
PKI	Public Key Infrastructure
PLC	Programmed Logic Controllers
PNNL	Pacific Northwest National Laboratory
ppb	parts per billion
PPE	Personal Protection and Equipment
PPO	Preferred Provider Organization
PPW	Partnership for Public Warning
PRA	Probabilistic Risk Assessment
R&D	Research and Development
R&R	Response and Recovery
R3S	Remote Surveillance Support System
RAP	Ring Airfoil Projectile
RDT&E	Research, Development, Test & Evaluation
REACT/S	Radiation Emergency Assistance Center/Training Site
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RHTCAT	Rapid High-Throughput Clinical Assessment and Testing (System)
RIMS	Response Information Management System
RISS-ATIX	Regional Information Sharing Systems – Anti-Terrorism Information eXchange

RISSNET	Regional Information Sharing System Network
RNA	Ribonucleic Acid
ROC	Regional Operations Centers
RPG	Rocket Propelled Grenade
RTO	Response Technology Objective
S&T	Science & Technology
SAIC	Science Applications International Corporation
SARC	Surveillance and Reconnaissance Center
SARS	Severe Acute Respiratory Syndrome
SART	State Animal Response Teams
SATURN	Statewide Anti-Terrorist Unified Response Network
SAW/IMS	Surface Acoustic Wave / Ion Mobility Spectrometry
SBCCOM	Soldier & Biological Chemical Command (Army)
SCA	Software Communications Architecture
SCADA	Supervisory Control and Data Acquisition
SCBA	Self-Contained Breathing Apparatus
SESI IR MS	Systems Engineering Solutions, Inc. Infrared Mass Spectrometry
SIGINT	Signals Intelligence
SIGP	Single Integrated Ground Picture
SIP	Single Integrated Picture
SLD	Second Line of Defense
SMART	Situation Management and Awareness in Real Time
SMO	Semiconducting Metal Oxides
SMPTE	Society of Motion Picture and Television Engineers
SNORT	Proper name of an open-source intrusion detection system
SONET	Synchronous Optical Network
SPAWAR	Space & Naval Warfare Systems Command (Navy)
SRA	Strategic Research Area
SWAT	Special Weapons And Tactics
T&E	Test and Evaluation
TACAS	Thermal Access Control and Authorization Systems
TACCS	Threat Analysis and Critical Control Point
TADMUS	Tactical Decision Making Under Stress
TASSS	Tulsa Area Syndromic Surveillance System
TD	Technology Demonstration
TEW	Terrorism Early Warning (Group)
TIC	Toxic Industrial Chemicals
TIGER	Team Integrated Electronic Response
TIM	Toxic Industrial Material
TRANSCOM	Transportation Command
TRC	Terrorism Research Center, Inc.
TRL	Technology Readiness Level
TSR	Technical Search and Rescue
TSWG	Technical Support Working Group
UAV	Unmanned Aerial Vehicle
UGS	Unattended Ground Sensors
UIC	Unified Incident Command Decision Support and Interoperable Communications
UNWD	Unconventional Nuclear Weapons Defense

UPS	United Parcel Service
USAMRIID	United States Army Medical Research Institute of Infectious Diseases
USAR	Urban Search and Rescue
USDA	United States Department of Agriculture
USMC	United States Marine Corps
UV	Ultraviolet
UWB	Ultra Wide Band
VLSTRACK	Vapor Liquid and Solid Tracking
VMAT	Veterinary Medical Assistance Teams
VR	Virtual Reality
VTC	Video Teleconferencing
WATS	Wide-Area Tracking System
WET	Weather, Enemy and Terrain
WETT	Weather, Enemy, Threats, and Terrain
WHO	World Health Organization
WMD	Weapons of Mass Destruction
XML	eXtensible Markup Language

Appendix C

Home Agencies of Project Participants And Interviewees

Congress

Subcommittee on Emerging Threats and Capabilities, Senate Armed Services Committee

Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform

House Republican Conference Terrorism Working Group

Executive Office of the President

National Security Council

Office of Homeland Security

Office of Management and Budget

Office of Science and Technology Policy National Security and International Affairs Division

Department of Homeland Security

Science and Technology Directorate

Emergency Preparedness and Response Directorate

Office of the Chief Counsel

Bureau of Transportation and Security Directorate, Office of Domestic Preparedness

National Domestic Preparedness Office

Plum Island Disease Center

National Emergency Training Center

National Bioterrorism Detection and Analysis Assessment Center

FEMA Senior Advisor for Terrorism

FEMA National Technology Transfer Center

FEMA WMD Resource Database

FEMA Urban Search and Rescue Massachusetts Task Force 1

Department of Justice

FBI Counterterrorism Division, Domestic Terrorism WMD Group

National Institute of Justice

FBI Laboratory

FBI Hazardous Materials Response Unit

Department of Defense

Interagency Board for Equipment Standardization and Interoperability

Technical Support Working Group

Office of the Undersecretary of Defense (Comptroller)

Deputy Assistant to the Secretary of Defense (DATSD) for Counterproliferation and Chem-Bio Defense (CP&CBD)

Office of the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)

Office of the Assistant to the Secretary of Defense for Civil Support

Joint Staff Deputy Directorate for Combating Terrorism (J-34)

Joint Forces Command Joint Task Force (Civil Support)

US Army Communications and Electronics Command

US Army Medical Research Institute of Chemical Defense

US Army Medical Research Institute of Infectious Diseases

US Army Soldier Biological and Chemical Command

US Marine Corps Systems Command

US Marine Corps Security Force Battalion

US Marine Corps Warfighting Laboratory

National Guard Bureau

Defense Advanced Research Projects Agency

Defense Threat Reduction Agency

Defense Intelligence Agency

National Defense University

Department of Energy

Sandia National Laboratories

Idaho National Engineering and Environmental Laboratory

Department of Commerce

National Institute of Standards and Technology, Office of Law Enforcement Standards

Department of State

Office of the Coordinator for Counter-Terrorism

Department of Health and Human Services

Centers for Disease Control and Prevention Bioterrorism Preparedness and Response Program

Food and Drug Administration, Center for Food Safety and Applied Nutrition

Department of Agriculture

Office of Crisis Planning and Management

Homeland Security Staff

Food Safety and Inspection Service (FSIS), Office of Food Safety and Emergency Preparedness

Animal Plant Health Inspection Service (APHIS)

Agricultural Research Service

Department of Transportation

Office of Emergency Transportation

National Academy of Sciences

Environmental Protection Agency

Central Intelligence Agency

State and Local Jurisdictions

Arlington County, VA, Fire Department

Baltimore MD Department of Health

Baton Rouge LA Coroner's Office

Baton Rouge LA Police Department

Boston Emergency Management Agency

Boston Emergency Medical Service

Boston Fire Department

Chicago Department of Public Health

Chicago Office of Emergency Management

City of Tulsa Department of Public Works

City of Tulsa Fire Department/HAZMAT Team

City of Tulsa Health Department

Commonwealth of Virginia Chief Veterinarian

District of Columbia Emergency Management Agency

District of Columbia Metropolitan Transit Police

Fairfax County HAZMAT Response Unit

Fairfax County Police Department

Fairfax County Urban Search and Rescue/ Virginia Task Force 1/USAID SAR Team 1

Fire Department of New York City

Fishers, IN, Fire Department

Harris County TX Department of Public Health

Illinois Department of Public Health

Kansas City MO Health Department

Los Angeles City Fire Department

Los Angeles Department of the Coroner

Los Angeles County Fire Department

Los Angeles County Sheriff's Department Emergency Operations Bureau

Los Angeles County Terrorism Early Warning Group

Los Angeles Police Department

Matteson, IL, Police Department

Metropolitan Boston Transit Authority

Miami/Dade County Office of Emergency Management

Miami/Dade County Urban Search and Rescue

Montgomery County Fire Department

North Carolina Department of Agriculture and Consumer Services, Emergency Programs Division

New Hampshire Office of Emergency Management

New York City Mayor's Office of Emergency Management

Oklahoma City Metropolitan Medical Response System

Oklahoma City/County Health Department

Orange County, CA, Sheriff Department of the Coroner

Pennsylvania Department of Agriculture

Pennsylvania Department of Health

Philadelphia Police Department

Pittsfield, MA, Fire Department

Redlands, CA, Police Department

San Diego Sheriff's Department

Salt Lake City Corporation Management Services Department

Salt Lake City Fire Department Special Operations Coordinator

Seattle Fire Department

Seattle Urban Search and Rescue/Metropolitan Medical Strike Team

Sheffield, MA, Police Department

South Carolina Law Enforcement Department

Utah Department of Health

Utah Department of Public Safety

Tulsa Area Emergency Management Agency

Private/Academic/Research Organizations

American Meat Institute

American Phytopathological Society

American Veterinary Medical Association

Auburn University

Aurora Safety

Banfield Pet Hospital, Fredericksburg, VA

Cactus Technology

Center for Strategic and International Studies

CMI-Services

Communications Applied Technology

Cornell University

Cugaar Software

Dartmouth University Media Labs

Defense Group Inc.

Drexel University

Federation of American Societies for Experimental Biology

GenCon, Inc.

Institute for Defense Analysis

Institute for the Study of Terrorism and Political Violence

International Association of Chiefs of Police

Lion Apparel

Louisiana State University

Maryland Institute for Emergency Medical Service Systems

McDonalds Corporation

MIT Lincoln Labs

MITRE

Monmouth University

Natick Labs

National Association of Emergency Medical Technicians

Monterey Institute of International Studies Center for Nonproliferation Studies

National Research Council

Nuclear Threat Initiative

OrthoOklahoma Healthcare

Radix Corporation

RAND Corporation

Sabiosi, Inc

Science Applications International Corporation

Southern Research Institute

Tex-Shield, Inc

Tulsa Hillcrest Health Care System

University of Kansas

University of Florida

University of Georgia at Griffin

University of Guelph, Canada

University of Maryland, Baltimore, National Study Center for Trauma and EMS

University of Nebraska

University of Pittsburgh Graduate School of Public Health

University of Texas at Austin Institute for Advanced Technology

University of Texas, San Antonio

University of Texas Medical Branch (Galveston)

Virginia Polytechnic Institute and State University

Washington State University

Appendix D

About the Authors and Editors

Guy Beakley, Ph.D., is Vice President of C4ISR for Hicks & Associates, Inc., senior scientist of the DoD/Intelligence Community Motion Imagery Standards Board, and a member of the SAIC Executive Science and Technology Council, a small group of scientists and technologists selected from SAIC and Telcordia as representative of the highest standards of technical quality. Recent programs he led include full-motion wireless video, voice and data communications system, International Telecommunication Union and NATO standards development, higher order protocols for Common Data Link, distance learning using optical fiber networks and satellites, and future imaging systems meeting the requirements of Joint Vision 2010. His current interests include high resolution systems for precision targeting, new technology compression systems, and broadband communications systems for urban and mobile environments. Prior to joining Hicks & Associates he was Director of Government Programs for Optivision, Inc., Vice President of Research and Development for Scientific-Atlanta, Inc. and Head of Image Processing Research at Sarnoff. He is a member of MPEG, IEEE, SMPTE, AFCEA, author of more than 60 papers and the recipient of the 1996 SMPTE Journal Award for most outstanding paper. Dr. Beakley received a B.E. in Electrical Engineering from Vanderbilt University and M.S., M.Phil., and Ph.D. degrees from Yale University in Engineering and Applied Science.

Thomas W. Frazier is the President of the National Consortium for Genomic Resources Management and Services (GenCon). Dr. Frazier is an experimental and physiological psychologist with a research and management background in aerospace and military biomedical research programs. Prior to creating GenCon, he was a biomedical research specialist at the Johnson Manned Spacecraft Center. He then came to Walter Reed Army Institute of Research where he became Chief, Department of Experimental Psychophysiology. He founded Behavioral Technology Consultants, Inc, which was a research, teaching, and consulting firm specialized in behavioral research and treatment programs, office automation technology development, and research on human stress and fatigue.

Now at GenCon, he has developed various conferences and workshops for senior professionals, and organized congressional briefings concerned particularly with issues confronting genomic researchers, administrators and legislators in the emerging threats arena. Through GenCon he has developed concept proposals for technology assessments investigating how to optimize surveillance and containment strategies through detection devices technology development. On emerging threats to food and agriculture, he has focused especially on emerging threats of radical environmental and animal rights organizations to modern U.S. agricultural biotechnology and to contemporary agricultural and food production processes and processor organizations.

Thomas M. Garwin is Vice President of Hicks & Associates, Inc., where he undertakes national security research and consulting tasks, primarily for the Departments of Energy and Defense. He has focused on counter-terrorism, counter-proliferation, defense transformation, and the health of the nuclear weapons stockpile. Before joining Hicks & Associates, Mr. Garwin served on the professional staff of the Committee on Armed Services of the U.S. House of Representatives. Mr. Garwin managed the full committee's hearings and developed policies on defense budgets

and force structure, military roles and missions, European and Asian security, and export controls. As a policy and economics advisor to Committee Chairman Les Aspin, Mr. Garwin helped formulate policy initiatives regarding post-Cold War national security strategy, military force posture, technology development, and defense conversion. Before joining the House Armed Services Committee, Mr. Garwin served as the American Coordinator of the Nuclear History Program at the University of Maryland. In this position, he oversaw the startup of a multimillion-dollar international research and training program. As a full-time consultant to the John D. and Catherine T. MacArthur Foundation from 1985 through 1987, Mr. Garwin helped define priorities, select grantees, and solidify support for the Foundation's $20 million-a-year International Security Program. Mr. Garwin previously served as an analyst with the U.S. Congressional Office of Technology Assessment from 1983 to 1985, where he managed research on the role of computation and communications in future U.S. economic growth. From 1981 to 1983, he was a researcher with the Brookings Institution, where he analyzed OPEC's role in oil markets and related national security issues. Mr. Garwin was a senior consultant to the Analytic Assessments Corporation from 1978 to 1983, where he invented "tagging" systems for arms control verification. He also analyzed intelligence collection systems and requirements, wartime command and control, and nuclear targeting issues. Mr. Garwin worked in the Office of the Assistant Secretary of Defense for International Affairs from 1976 to 1977, where he represented the Office of the Secretary of Defense on National Security Council Task Forces concerning defense strategy, technology, and arms control. Mr. Garwin holds a Master of Public Policy from Harvard University's John F. Kennedy School of Government and an A.B. degree in History from Harvard College. In 1994, Mr. Garwin returned to the Kennedy School to attend the Program for Senior Executives in National and International Security.

James Hammill is Vice President for Government Special Projects at Telcordia Technologies, where he supports public sector projects related to Telcordia's core telecommunications and IT functions. Mr. Hammill represents Telcordia as a member of the FCC's National Reliability and Interoperability Committee (NRIC-VI), Homeland Security Public Safety Committee; and through the MITRE Corporation, represents Telcordia in the Partnership for Public Warning, which will become a Federal Advisory Committee for the standardization of emergency warning for the United States. In this capacity, Mr. Hammill serves as chair of the Operating System Standards Committee for Public Warning Technology, and co-chair of the Standards Terminology Committee.

Hal Kempfer of Knowledge & Intelligence Program Professionals (KIPP) is a public and private sector intelligence professional with over fifteen years of experience in the field. Involved with business intelligence since 1992, Hal has had subsequent lengthy engagements involved with cutting-edge law enforcement and military intelligence program initiatives. Lieutenant Colonel Kempfer, U.S. Marine Corps Reserve, completed a tour overseas last year as the Director of Intelligence (J-2) of the Combined Joint Task Force for Consequence Management, and is currently the Marine Emergency Preparedness Liaison Officer for California, Arizona, Nevada and Hawaii. KIPP is teamed with leading companies in the area of competitive intelligence and strategic risk management with a variety of clients in government and industry. Hal currently appears on ABC 7 television and NPR radio in Southern California as a military and terrorism analyst, and lectures at the National Interagency Civil-Military Institute.

Dr. Steven Kornguth is currently the Director of Chemical and Biological Defense at the Institute for Advanced Technology and visiting Professor of Neurobiology at the University of Texas at Austin. Dr. Kornguth is Principle Investigator on the University of Texas Component of the Biological Chemical Countermeasures Effort of a National Consortium. He has research activities in sensors, magnetic resonance imaging

and human performance. Dr. Kornguth has a B.S. Chemistry from Columbia University, a M.S. in Biochemistry and Ph.D. Biochemistry from the University of Wisconsin, Madison.

Mr. Brett Kriger was Deputy Director of the Louisiana Office of Emergency Preparedness from 1990 to 1997. He has over 30 years of domestic and international military and civilian experience in all aspects of planning, training, and exercise development and evaluation for all-hazards including: national security, CBRNE accidents/incidents, nuclear weapon accidents, nuclear power plants, industrial chemicals, and terrorist attack. He is an expert in emergency response and has coordinated planning teams to develop WMD incident management plans, was a Team Leader for the National Guard WMD Study, and a member of the planning team and a player/controller for the FBI series of Improvised Nuclear Device exercises held prior to the Atlanta Olympics. He assisted in the development of the initial guidelines for the Chemical Stockpile Emergency Preparedness Program and serves as a Regional Coordinator and Team Leader for FEMA's Radiological Emergency Preparedness Program. He is a nationally recognized expert in WMD planning and response with extensive qualifications in developing state and local terrorist incident response capabilities.

Jasper C. Lupo, Ph.D., is Director of Sensor Systems and Principal Scientist at Applied Research Associates, Inc. He leads ARA programs in the areas of space and defense, especially sensor initiatives. Dr. Lupo is a senior technologist with over thirty years experience in conducting and leading defense research and development, from the laboratory to the Office of Secretary of Defense. This experience is mainly in science and technology, but spans the range from basic research to early production. Many of his projects have been fielded or been incorporated into fielded military systems. From 1996 to 2001 he served as Director, Sensor Systems, Office of the Deputy Undersecretary of Defense (OSD) for Science and Technology, where he managed the $1.4B Department of Defense (DoD) science and technology investment in sensors, electronic components, electronic warfare, space platforms, space propulsion, medical sensing, and space sensors. From 1993 1996 he served as Director for Research, in the Office of the Director, Defense Research and Engineering, where he managed the $1.1B Department of Defense (DoD) Basic Research Program, chaired the Defense Committee on Research, managed the DoD Multidisciplinary University Research Program, and established the DoD Strategic Research Objectives and first Basic Research Plan. Before joining OSD, he was Assistant Director for Smart Weapons, Tactical Technology Office, Defense Advanced Research Projects Agency (DARPA). He directed programs in smart weapons, sensor development, sensor processing, and automatic target recognition; he also chaired the DARPA Neural Network Study. Dr. Lupo has a Ph.D. in Physics from Georgetown University.

John W. Lyons, Ph.D., is a physical chemist, technology consultant, retired director of the Army Research Laboratory (ARL), and member of the National Academy of Engineering. He served in research and development positions with the Monsanto Company for 18 years. In 1973 he joined the Commerce Department's National Bureau of Standards (NBS). At NBS, Lyons was the first director of the Center for Fire Research. In 1990, Dr. Lyons was appointed by President George H.W. Bush to be the ninth director of NBS; by that time renamed the National Institute of Standards and Technology (NIST). In September 1993, he was appointed the first permanent director of ARL. At ARL, Dr. Lyons managed a broad array of science and technology programs. He has served on many boards and commissions, to include the Federal Advisory Commission on Consolidation and Conversion of Defense Research and Development Laboratories. He currently serves on two boards of visitors at the University of Maryland. He is a member of the National Research Council's Board on Army Science and Technology, as well as a member of a congressionally chartered committee at the National Defense University to study the potential effectiveness of the DoD laboratories in the

transformed military of the future. Dr. Lyons was elected to the National Academy of Engineering in 1985. He is a Fellow of the American Association for the Advancement of Science and of the Washington Academy of Science, and is a member of the American Chemical Society and of Sigma Xi.

LOU MASON is Director of Logistics Transformation at the Hicks & Associates Advanced Systems and Concepts Office. Prior to arriving at Hicks & Associates, he was the DARPA Program Manager for the Logistic Advanced Concept Technology Demonstrations, including the Joint Logistics ACTD and the Joint Theater Logistics ACTD, with the mission to develop and integrate web-based Joint Logistics Decision Support Tools (JDSTs) into the Global Combat Support System. Several of his products are currently being integrated into the GCSS CINC/JTF and Army Logistics Transformation Agency programs. Lou came to DARPA from MITRE Corporation, where as a Senior Lead Engineer, he was the GCSS Task Lead for the DARPA/DISA Joint Program Office (JPO). He is a retired Army logistician with over 36 years experience in strategic and operational planning, analysis, and logistic systems integration. He has extensive joint logistics and Special Operations experience, and has authored key joint logistics doctrine. While on active duty in the Army, he served as the Director of Operations for the Army Material Command, the Deputy Chief of Staff for Logistics U.S. Army Special Operations Command, Commander of the Special Operations Support Command, Chief of Organization and Mission Defense Logistics Agency, and Chief of Supply Systems U.S. Forces Korea. Lou has supported numerous DARPA projects, including the Logistics for the Warrior Program, the Logistics Anchor Desk, and the Advanced Logistics Program (ALP). He is a graduate of the Army War College and the Army Command and General Staff College. Lou is also a graduate of the University of Southern Mississippi, and holds advanced degrees from Georgia State University and the University of North Alabama.

MICHELLE ROYAL is Director for Strategic Planning at Hicks & Associates, Inc., where she supports technology planning for the Memorial Institute for the Prevention of Terrorism (MIPT), and the Border and Transportation Security Administration within the Department of Homeland Security (DHS). Prior to joining Hicks & Associates, Inc., Ms. Royal was a Project Director at Science Applications International Corporation, where she was responsible for program management of a number of projects, including a market survey and analysis of the high explosives market (to include DoD, foreign, and private industry procurement and demilitarization), DoD ODISC4 Smart Card/Common Access Card/Public Key Infrastructure analytical support, and an assessment of the U.S. solid rocket-motor propellant market for a foreign propellant manufacturer. In addition to program management duties, Ms. Royal supported the development of technology roadmaps for the Air Force Research Laboratory (AFRL). Prior to joining SAIC, Ms. Royal was an Intelligence Research Specialist for the Federal Bureau of Investigation, where she conducted research and analysis for foreign counterintelligence operations. Ms. Royal has a B.A. in International Relations and Italian, an M.A. in Security Policy Studies, and an M.B.A. from The George Washington University.

NEAL A. POLLARD, J.D., is Vice President, Emerging Threats & Capabilities, at Hicks & Associates, Inc., where he leads Project Responder, as well as consults on numerous government projects as a terrorism expert, technology planner, and national security lawyer. Mr. Pollard has over twelve years of experience in researching terrorism and transnational threats, and eight years' experience developing counterterrorism strategies and plans. In 1996, Mr. Pollard co-founded the Terrorism Research Center, Inc. (TRC), an institute with representation in seven countries worldwide, and dedicated to research and analysis of terrorism, counterterrorism policy and strategy development, and public information and education. Mr. Pollard continues to serve on the TRC Board of Directors.

Mr. Pollard holds degrees in mathematics and political science, an M.Litt. in International Security Studies from the University of St. Andrews, Scotland, and a Juris Doctor cum laude from the Georgetown University Law Center, where he specialized in international and national security law.

Maria E. Powell, Ph.D., is a Senior Director with the Terrorism Research Center. Her main portfolio includes work with the emergency responder community and technologists to define requirements, priorities, and roadmaps in order to develop a national technology planning process for capabilities to respond to terrorism; and to develop a model of the Terrorism Early Warning Group concept that can be tailored and replicated in other local jurisdictions. From 1997-2003, Dr. Powell was a Project Analyst/ Director with Science Applications International Corporation where she specialized in terrorism, nuclear strategies, biological technologies, non-lethal weapons, and the Revolution in Military Affairs. Dr. Powell has also worked on demining issues in the Department of Humanitarian Affairs of the United Nations in New York, and was a member of a delegation to a preparatory conference in Geneva for the Convention on Certain Conventional Weapons. Dr. Powell received a B.A. in Russian and Political Science from Allegheny College, and an M.Phil. and Ph.D. in International Relations from the University of St. Andrews, Scotland, where she focused on terrorism, police and intelligence cooperation to combat terrorism in the European Community, and the interplay between international humanitarian law and arms control in the context of the landmine and chemical weapons regimes.

Barbara Reagor, Ph.D., is Vice President for Homeland Security and Government Markets, at Telcordia Technologies. Dr. Reagor has worked for the last 33 years in the fields of Broadband Networking, Enterprise Management Solutions, e-Business Solutions, Community Notification (Reverse 9-1-1), Disaster Prevention & Recovery, Crisis Management, Chemical Contamination, Network Reliability and Network Risk Assessment associated with telecommunications and information technology systems. For more than 26 years, Dr. Reagor and her department worked on such events as World Trade Center Bombings, Pentagon Bombing, Mt. Saint Helens, Hurricane Andrew, the Hinsdale Fire, the Northridge Earthquake, the Oklahoma City Federal Building Bombing and many more disasters associated with fires, floods, hurricanes, earthquakes, and dust storms. She has been the Telcordia Spokesperson for Homeland Security and Critical Infrastructure Protection since the September 11th Terrorist Attacks, and is coordinator of the Telcordia Task Force in support of the U.S. Governments Homeland Security initiatives. Over the past 3 years, Dr. Reagor lead the research, development and commercialization of an advanced messaging platform ideally suited for Public Safety Notification for large and small-scale emergencies, including hurricanes, floods, gas leaks and missing children. She is currently on the Interim Board of Directors for a newly forming FACA organization called the "Partnership for Public Warning." Dr. Reagor has a B.Sc. in Chemistry, an M.S. in Organic Chemistry, and a Ph.D. in Inorganic Laser Chemistry from Seton Hall University.

Robert V. Tuohy is Vice President for Strategic Planning at Hicks & Associates, Inc. Since coming to Hicks, Mr. Tuohy has been advising several government and non-government organizations on technology planning. Besides leading the development of Project Responder's National Technology Plan for Responding to Terrorism, he is also assisting the Department of Homeland Security in developing processes for addressing their Border & Transportation Security technology needs. Prior to joining Hicks & Associates, Mr. Tuohy served as the Director of Science and Technology Plans & Programs in the Office of the Secretary of Defense. Mr. Tuohy was responsible for developing and coordinating the Department's science and technology strategic planning and program assessment activities. Mr. Tuohy has a B.A. in Applied Behavioral Sciences from National-Louis University, and an M.S. in Science and Technology Commercialization from the University of Texas at Austin.

Appendix E

Index