Department of Homeland Security
Critical Infrastructure Protection

Report of Federal Research Leaders Workshop

16 December 2004 Session Report
Final

January 2005

Table of Contents

INDEX OF FIGURES

INDEX OF TABLES

ACRONYMS

CI	Critical infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
DHS	Department of Homeland Security
HSPD	Homeland Security Presidential Directive
ISC	Infrastructure Sub-Committee
IWG	Interagency Working Group
KR	Key resource
NCIP R&D Plan	National Critical Infrastructure Protection Research and Development Plan
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PS&S	Physical Structures and Systems
R&D	Research and Development
S&T	DHS Science and Technology Directorate
SME	Subject Matter Expert

1.0 EXECUTIVE SUMMARY

The events of September 11th, 2001 forever changed how the Nation thinks about Homeland Security. Assumptions about the Nations relative immunity to terror events were shown to be false. The security of US citizens and protection of US assets is of utmost importance and requires a significant shift in homeland security policies.

In response to protecting US assets and formulating more robust policies, the Administration created Homeland Security Presidential Directive 7 (HSPD-7), dated December 17, 2003. The directive specified that the "Office of Science and Technology Policy, in coordination with the Department (DHS), will coordinate interagency research and development to enhance the protection of CI and key resources".[1] To support this mandate, the White House Office of Science and Technology Policy (OSTP) and the Department of Homeland Security (DHS) jointly sponsored a workshop of Federal agency technical program managers in the area of Critical Infrastructure Protection (CIP) Research and Development (R&D). This workshop, organized through the Infrastructure Subcommittee of the National Science and Technology Council, was held on December 16, 2004 at the Sheraton Hotel in Crystal City (Arlington), Virginia. The workshop represented the first in a series of workshops to address important issues for technical managers from all Federal agencies involved in CIP R&D.

The workshop was organized into three distinct portions: **Context Setting**, **Mapping**, and **Priorities**. Context setting offered workshop participants an opportunity to hear from leaders who's Agencies have a key role in CIP R&D and also to hear about efforts currently underway, such as the NCIP R&D Plan. Mapping provided an opportunity for attendees to provide insight into how current work in CIP R&D aligns to the 2004 NCIP R&D Plan. The priorities portion of the workshop allowed Federal R&D Leaders to come to consensus on priorities for future CIP R&D.

The Keynote speakers included Dr. John Brighton, National Science Foundation, Dr. Hratch Semerjian, National Institute of Standards and Technology (NIST), Dr. Charles McQueary, DHS, and Dr. John Marburger, OSTP. Each speaker provided his perspective on the state of Homeland Security and more specifically the importance of CIP R&D to protecting the Homeland. Each leader also articulated his support for participation in the first Federal R&D Program Manager workshop to help meet the goals of HSPD-7.

During the mapping portion of the day, workshop participants heard about the efforts underway to meet HSPD-7. Dr. John Cumming's, the CIP Portfolio Manger within DHS S&T, provided an overview of the NCIP R&D Plan, noting that the plan is organized around themes, as opposed to sectors. The NCIP R&D themes are:

- Detection and sensor systems
- Protection and prevention

[1] Homeland Security Presidential Directive – 7; Critical Infrastructure Identification, Prioritization, and Protection. December 17th, 2003.

- Entry and access portals
- Insider threats
- Analysis and detection support systems
- Response, recovery and reconstitution
- New and emerging threats and vulnerabilities
- Advanced infrastructure architecture and systems design
- Human and social issues
- Other

The priorities portion of the day focused on agency representatives and invited participants to experience the challenge of meeting HSPD-7. Agencies were asked to do what they do regularly: identify their agencies CIP R&D priorities. Participants then met in interagency tables where they were asked to come to consensus on what the Nation's priorities should be in R&D to protect CI. Interagency tables then engaged in facilitated conversation to defend and create the top priorities for CIP R&D:

- Resilient, self-healing, self-diagnosing, adaptive, damage limiting, physical, biological and cyber human infrastructure systems
- National Common Operating Picture
- Secure National Communication Network
- Technology monitoring and forecasting intellectual capital the movement of technology
- Human and Social Issues
- Access to information about sensitive, complex systems and validation techniques of complex models.

During the final portion of the priorities exercise, interagency tables had the opportunity to "act as if they were OMB" to advise the President on where CIP R&D resources should be allocated. The results of the exercise demonstrated alignment with priorities currently outlined in the 2004 NCIP R&D Plan and also validated a relatively high concurrence among the top three highest priorities. The top three priorities as identified by the meeting participants were:

- Resilient self-healing systems
- National Common Operating Picture
- Secure National Communication Networks.

The workshop concluded with a collective sense of how important it is for Federal Agencies to work together in support of R&D to protect CI. Many participants made valuable connections with colleagues working on similar issues in other agencies and noted their appreciation for the opportunity to network with colleagues and other Program Managers from across the Federal government. Dr. John Cummings noted there will be a workshop with CI owner/operators to hear their perspectives about CIP R&D and he also highlighted the need for a follow-on Federal R&D Program Manager workshop as well as a workshop with Academe and other R&D providers as part of 2005 NCIP R&D Plan efforts.

2.0 INTRODUCTION

The Nation's critical infrastructure is broad and at risk to terrorist attacks. DHS has identified 17 critical infrastructures and key assets/icons. They include such sectors as: Banking and Finance, Telecommunications, Food, Agriculture, Water, Public Health, Transportation, Energy, and others. In addition, individual assets make up the CI sectors and must be protected. The Agricultural sector alone includes 1,912,000 farms and 87,000 food processing plants. The Energy sector includes 2,800 electric power plants, 104 commercial nuclear power plants, 300,000 producing oil and natural gas sites, and 2,000,000 miles of pipeline.

If the scope alone of identifying what research and development must be done to protect these assets is not daunting enough, consider that while the government is helping to protect the Nation's Critical Infrastructure, 85 percent of which is owned by private Industry and state and local officials. Combine that with legal and policy issues that often make it difficult to share information [e.g. Federal Advisory Council Act (FACA) and Freedom of Information Act (FOIA)], the strong parochial interests among individual agencies to protect their own missions, the inherent need to include the academic community in R&D, and there is a real challenge!

2.1 Background

In response to meeting the CIP R&D challenge, the Administration created HSPD-7 dated December 17, 2003. The directive specified that the "Office of Science and Technology Policy (OSTP), in coordination with the Department (DHS), will coordinate interagency research and development to enhance the protection of critical infrastructure and key resources".[2]

The DHS S&T Directorate is the research and development arm of DHS. Its priority is to find technology solutions to meet pressing homeland security challenges. S&T is specifically tasked with marshalling the intellectual capital of the engineering and scientific communities to develop approaches to safeguard the American public. In this role, DHS S&T was uniquely qualified to lead the effort to meet the mandate set forth in HSPD-7. S&T initiated steps to plan and coordinate R&D efforts across Agencies and critical infrastructure sectors. The result was the first ever National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan).

The 2004 Plan laid the foundation for what will become an annual report outlining National CIP R&D requirements and the Federal government's plan to address these requirements. The responsibility for leading the preparation of this interagency plan was shared between DHS and the White House OSTP. The OSTP National Science and Technology Council's Infrastructure Sub-Committee (ISC) provided the interagency forum for preparing this plan, gathering Subject Matter Expert (SME) recommendations, and reviewing the results.

[2] Homeland Security Presidential Directive – 7; Critical Infrastructure Identification, Prioritization, and Protection. December 17th, 2003.

The Federal government will use the initial NCIP R&D Plan as a baseline from which to develop future year plans and eventually to allocate and schedule federal R&D resources in support of CIP. Work carried out under this NCIP R&D Plan will inform and persuade people impacted by CIP, establish the accountability for specified results, and enable decision-making.

The first Federal Research Leaders Workshop, held on December 16th, 2004 supports the mandate described in HSPD-7 to coordinate Federal Critical Infrastructure Protection Research and Development. The following report provides a summary of the workshop.

2.3 Purpose of the Federal Research Leaders Workshop

On December 16th 2004, over 110 Research Leaders (Appendix D) from approximately 30 Agencies across the Federal government came together with the purpose of "aligning government leaders with a shared understanding of the scope, purpose, approach, and coordinated actions focusing on R&D to secure critical infrastructures".

The desired outcomes from the workshop were to:

- Develop a shared understanding of the scope included in the 2004 National CIP R&D Plan and linkages to other homeland security R&D plans
- Develop a shared understanding of Federal critical infrastructure protection technical programs
- Clarify R&D efforts underway and identify opportunities to collaborate in order to better protect critical infrastructure
- Introduce priorities identified in the 2004 National CIP R&D Plan
- Develop an initial framework for the 2005 NCIP R&D Plan using 2004 priorities as a foundation
- Establish a program manager community of interest for connectivity and collaboration.

A core team comprised of representatives from OSTP, DHS, NIST, and NSF, along with members of Touchstone Consulting developed an agenda to accomplish these workshop outcomes/objectives. The high level agenda is included as Appendix A and the primary agenda topics included:

- An explanation of the meeting purpose and outcomes
- Setting context for CIP R&D
- Mapping of current agency programs
- First Glimpse of 2005 CIP R&D Priorities
- Next steps.

The overall tone of the Federal Research Leaders Workshop was set up to be collaborative and participants agreed to a set of guiding principles at the meeting outset (Figure 1). During the day, participants were asked to consider different perspectives. For instance, as representatives of their Agencies, participants were asked to use "little hat thinking" and as representatives of the Federal government and as citizens of the United States, to use "big hat thinking" (Figure 2). Mutual respect and admiration was apparent between participants who also agreed to a working definition of consensus (Figure 3). Generally speaking, the meeting was considered a success by participants.

Figure 1 - Guiding Principles

Figure 2 - Big Hat versus Little Hat Thinking

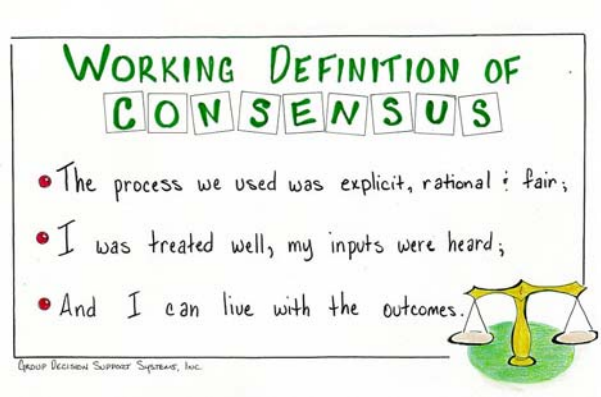

Figure 3 - Working Definition of Consensus

2.4 How this Document is Organized

This report is organized into three major sections following the order of the workshop agenda: Context, Mapping, and Priorities. The report captures, at a high level, discussions and key points from the workshop. Where appropriate, data resulting from breakout groups and exercises is reflected in the body of the report. Additional information, such as presentations, attendance lists, data sheets, etc. is included in the Appendices.

3.0 CONTEXT

Given that the scope for CIP R&D is expansive and touches almost every federal department, the Federal Research Leaders Workshop on CIP was organized as a venue where a diverse group of Federal Program Managers and researchers could begin to get to know each other and start to build a community of interest around CIP R&D. To this end, the discussions and activities of the day facilitated interagency and intra-agency discussions and debates and encouraged expanding individuals' networking groups across agency lines.

3.1 Keynote Speakers

As the primary organizing Agencies behind the workshop, NSF, NIST, DHS, and OSTP provided keynote speakers. The speakers shared their Agency's perspectives on the homeland security R&D arena, the 2004 NCIP R&D Plan, and articulated support to workshop attendees for their participation in meeting HSPD-7.

The keynote speakers included:

- Dr. John Brighton, Assistant Director for Engineering, NSF
- Dr. Hratch Semerjian, Acting Director, NIST
- Dr. Charles McQueary, Under Secretary for S&T, DHS
- Dr. John Marburger, Director, OSTP

Summaries of each speaker's comments are below, in the order in which they addressed the workshop participants.

3.1.1 Dr. John Brighton.

Dr. John Brighton, NSF, began by sharing that NSF's commitments to the homeland security mission were to collaborate, work within the community, and work to achieve an end goal by following an established roadmap. Dr. Brighton went on to speak about the 2004 NCIP R&D Plan, commenting that he was pleased with the structure and division of the plan into thematic areas as it recognizes the interdependencies and mutual needs within CI sectors. He went on to explain that true success of homeland security R&D efforts would enable innovation and foster development. In conclusion, he offered that from his perspective, the real purpose of the workshop was to find and make the connections with the other people in the room in order to begin to build a community around CIP R&D.

3.1.2 Dr. Hratch Semergian.

Dr. Hratch Semerjian, NIST, highlighted the roles of many Federal agencies in protecting our homeland, and emphasized that NIST is dedicated to contributing to the promotion and development of standards and to ensure that new technologies can work together throughout the various stages of development. Furthermore, he discussed the importance of HSPD-7 in setting the policy for developing a roadmap for CIP R&D, which he views as a vital next step in helping to safeguard the nation.

3.1.3 Dr. Charles McQuearly.

Dr. Charles McQueary, DHS, expressed his hopes that the workshop would be the first step towards increased communications and partnering that would help leverage existing resources to sustain technology development to protect the homeland. He noted that this was especially important to DHS given that they are heavily dependent upon interagency coordination. Although Dr. McQueary acknowledged that there is much work to be done in CIP R&D, he characterized the first iteration of the Plan as a strong foundation from which to build future year's efforts.

3.1.4 Dr. John Marburger.

As the final speaker, Dr. John Marburger, OSTP, began by echoing the message provided by the other speakers before him, that all federal agencies have a role in helping to secure our Nation and that they must all collaborate in order to be successful and the workshop was a step in that direction. He also stated that he was pleased with the iterative and collaborative processes used to develop the 2004 Plan and its themes and maintained that the Plan was on the right track to be used as a guiding document. Dr. Marburger concluded his comments by advising that the participants keep the bigger picture of homeland security in mind and remain aware of the other efforts that feed into future CIP R&D work.

3.2 Overview of HSPD-7 and the NCIP R&D Plan

To support participants in understanding the context around CIP R&D and to prepare participants for the afternoon portion of the workshop, Dr. Cummings provided overviews of HSPD-7, including the National Infrastructure Protection Plan (NIPP), as well as the 2004 NCIP R&D Plan. A summary of the overview follows:

HSPD-7 and NIPP

Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, was released on December 17, 2003 and outlines the requirements for protecting the nation's critical infrastructure. With this directive, the President established a national policy for Federal departments and Agencies to identify and prioritize United States CI and key resources (KR) and to protect them from terrorist attacks.

The directive mandated the development of the National Infrastructure Protection Plan (NIPP). The purpose of the NIPP is to provide the mechanism for establishing a dynamic, integrated, National Critical Infrastructure Protection Program that reduces vulnerability of CI/KR to terrorist

attacks through identification of CI/KR threats and assets, assessment and prioritization of CI/KR vulnerabilities, and the development and implementation of protection programs.

By means of HSPD-7, the country's homeland security effort was directed toward protecting the CI sectors and key assets identified as: Agriculture, Food, Water, Public Health, Emergency Services, the Defense Industrial Base, Information Technology, Telecommunications, Energy, Transportation, Banking and Finance, Chemical Industry and Hazardous Materials, Postal and Shipping, National Monuments and Icons, Dams, Government Facilities, Commercial Facilities, and Nuclear Reactors, Materials and Waste.

2004 National Critical Infrastructure Protection Research & Development Plan

HSPD-7 also mandates that an annual National Critical Infrastructure Protection Research and Development Plan be developed by DHS and the White House OSTP. Section 22 (e) states that:

> *"In coordination with the Director of the Office of Science and Technology Policy, the Secretary [DHS] shall prepare on an annual basis a Federal Research and Development Plan in support of this directive [Critical Infrastructure Identification, Prioritization, and Protection]"*

The NCIP R&D Plan will be developed and updated annually by the National Science and Technology Council (NSTC) and the ISC, which reports to the Committee on Homeland and National Security and the Committee on Technology. The ISC is supported by two Interagency Working Groups (IWGs) in this planning effort, namely Physical Structures and Systems (PS&S) and Critical Information Infrastructure Protection (CIIP). The annual NCIP R&D Plan will integrate R&D efforts across the physical and cyber domains. Furthermore, the Plan will address R&D programs and requirements across Federal agencies, and, to the extent practicable and in the best interests of the Nation, the requirements of the CI sector owners and operators as well as those of international organizations.

NCIP R&D Themes and Characteristics

The 2004 NCIP R&D Plan is structured around nine science, engineering, and technology themes. The themes were developed with input from over 200 Federal stakeholders working in the CIP R&D arena. The themes focus on the major efforts required to reduce vulnerabilities, increase protection, and speed recovery that position us to adopt proactive, strategic, long-lasting measures rather than simply reacting to the latest threat. The Plan is organized in themes with common characteristics, rather than sectors, that cross-cut multiple Agencies efforts, include long & short-term goals, and involve hard and soft sciences. Furthermore, the themes link to the areas of Intelligence, Weapons of Mass Destruction (Chemical, Biological, Radiation, and Nuclear), Law Enforcement, First Responders, and Standards that they are either dependent or reliant on in order to be successfully developed. The themes are:

- Detection and Sensor Systems
- Protection and Prevention
- Entry and Access Portals
- Insider Threats
- Analysis and Decision Support Systems

- Response, Recovery and Reconstitution
- New and Emerging Threats and Vulnerabilities
- Advanced Infrastructure Architectures and Systems Design
- Human and Social Issues

In addition to the themes, three over-arching strategic goals were developed that focus on the future of CIP R&D. The Plan lays out initial recommendations of CIP R&D that work toward these strategic goals to provide maximum value for the investment made by the Nation and to provide maximum security and resilience within and across infrastructure sectors. The strategic goals are:

- A national common operating picture for critical infrastructures
- An inherently secure next-generation Internet architecture
- Resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems

At the time of the workshop, the draft of the 2004 NCIP R&D Plan was near final release awaiting approval and signature from DHS and OSTP. The 2004 Plan will be shared with the private sector as well as other non-Federal government organizations. The information from the workshop will be incorporated into the 2005 draft, which will build on the foundation and ideas of the 2004 Plan. The F2005 Plan will include increased owner and operator input, specific milestones, budgets and deliverables. To achieve this, the CIP R&D Portfolio Management office will host an Industry Workshop, another Federal Program Management Workshop, and an R&D Providers Workshop. A draft of the 2005 NCIP R&D Plan will be distributed for Agency review and comment through the ISC as it is developed.

3.3 Breakout – Questions and Answers

Workshop participants had an opportunity to ask questions they had based on the context setting and specifically around the 2004 NCIP R&D Plan. Below are key questions from participants. Additional answers are included in Appendix B.

1. *What is and isn't Critical Infrastructure?*
    a. From the Homeland Security Act and HSPD-7, critical infrastructures are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. This includes everything from water and food infrastructures, to transportation, finance, and a dozen other areas, including the ubiquitous cyber security and information network infrastructure. What is not CI requires a more flexible definition based on a specific infrastructure and its components. For example, CIP does not have responsibility to develop the sensor technologies for detecting malevolent biological agents in our water, food, air environments – rather, CIP is responsible for the deployment and integration of these new technologies in a manner that maximizes their effectiveness while remaining interoperable with larger or adjunct systems.

2. *When does industry, including owner and operator and the industry that supplies them, start coming into the 2005 CIP R&D?*
    a. An industry workshop with the R&D representatives is planned for February or Spring 2005.
    b. DHS is partnering with the Sector Coordinating Councils and the Information Sharing and Analysis Centers (ISAC)[3]
    c. First, we need the have the 2004 NCIP R&D Plan signed and in the public domain
    d. In 2005, the National Plan will include a R&D roadmap that will coordinate with private industry, specifically on issues related to commercialization

3. *Do the themes in the NCIP R&D Plan cover what the group (Federal Government) is doing? Is there a prioritization of themes and priorities? How are we going to focus the topics in Plan?*
    a. The 2004 NCIP R&D Plan was developed by members (and other designees) of the ISC of the NSTC. The ISC membership includes 23 Federal agencies, most of which are participating in this workshop. In general, the 2004 NCIP R&D Plan is representative of the R&D work performed in the Federal agencies, but is not necessary complete. The selection of the themes and prioritization of the main objectives represent the best efforts of the ISC working these issues over the last year. One of the goals of this workshop is to vet the themes and priorities, adjusting each as appropriate prior to developing the 2005 National NCIP R&D Plan. We anticipate, based on a broader range of stakeholder input, that the 2005 Plan will be more focused and better aligned with national priorities in CIP.

4. *What is the game plan? How do we get agencies to work together?*
    a. One of the fundamental challenges in Homeland Security environment is to develop better federal agency cooperation. Key to addressing this challenge is a mutual

[3] The Sector Coordinating Councils are policy-level organizations charged with representing a sector strategy for addressing infrastructure protection. They work with Government Coordinating Councils to identify needed initiatives and timelines for implementation - and usually work with ISACs to disseminate information on the latest homeland security issues, like terror threats.

understanding of the goals, objectives, and as importantly, the challenges in their implementation. With federal agencies facing increasingly tight budgets, better collaboration, partnering and leveraging resources are required. In the 2006 budget cycle, OMB will have a separate line item in the President's budget representing the Federal agency programs in homeland security and infrastructure protection and will provide a first definitive step toward better planning and execution.

5. *Who are the customers of the NCIP R&D Plan?*
    a. The primary customers are the owners and operators of the nation's CI[4]. The stakeholder community for CIP is much larger: the Federal, state and local governments also have responsibility to protect government operations, the economy, and the American people from the effects of failures to our infrastructures. The vendor community represents a customer base in making available effective commercial products and technologies to protect CI across a broad range of applications.

6. *How do you spur basic research to the CIP objectives?*
    a. While basic research is the providence of both the Federal and private sector, traditionally for areas of broad application or long-term/deferred payback, the Federal R&D enterprise often takes the lead role. Federal funding for CIP R&D requires a strong, well-organized research and development plan. The NCIP R&D Plan is precisely the vehicle that Congress and OMB intended to provide such direction and coordination.

7. *How will CIP results be shared?*
    a. We expect that the 2004 National CIP R&D Plan will be publicly available in February 2005. In the Spring, a workshop with industry representatives will use the results from the plan and this workshop as a basis for their discussions. Similarly, a future workshop is envisioned focused on researchers from academe, national laboratories, and the broader R&D and homeland security communities.

8. *How do HSPDs 7, 9, 10, & 11 relate to each other?*
    a. Cyber and Physical are interlocked in the plan
        i. They are in the plan as Interlinking puzzle pieces in the puzzle.
    b. HSPD 9 establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
    c. HSPD 10 "BioDefense for the 21st Century " is a classified directive that establishes a national policy along the lines of the Biowatch program
    d. HSPD 11 is responsible to i) enhance terrorist-related screening through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security and to ii) implement a coordinated and comprehensive approach to terrorist-related screening.

[4] It is estimated the 85% of the critical infrastructure is in the private sector

3.4 Panel of CIP-related Portfolios

In order to highlight the linkages and interconnected nature of the work that is already underway for homeland security and CI protection across DHS and other agencies, a panel of speakers was assembled to address the workshop participants. The panelists represented a diverse set of interests with a common bond relating to CIP and shared their experiences with emergency preparedness and response (EP&R) and countermeasures for biological, chemical, radiological, and nuclear threats.

The agency Portfolio Manager panelists included:

- Dr. John Vitko, DHS Biological Countermeasures
- Dr. Tim Oppelt, Environmental Protection Agency (EPA) Biological and Chemical Countermeasures
- Dr. Randy Long, DHS Chemical Countermeasures
- Mr. Brooke Buddemeier, DHS Emergency Preparedness and Response
- Dr. Laurie Waters, DHS Radiological and Nuclear Countermeasures.

Their collective message served to paint the picture that CIP is only one element of the total homeland security landscape and that there are vast opportunities for collaboration and cooperation across agencies.

The following paragraphs summarize the information presented by the panelists. Please refer to the supplemental materials for the panelists' presentations.

3.4.1 Dr. John Vitko, Jr.

Dr. Vitko offered his perspective on the highest priorities related to R&D within the DHS portfolio of Biological Countermeasures. He underscored his participation in various interagency committees dealing with activities such as the implementation of HSPD-9 and 10, developing a joint R&D strategy for defense against agro-terrorism, and working with programs for bio-surveillance and monitoring, which demonstrated the collaborative nature of the Biological Countermeasures portfolio.

Dr. Vitko described the Biological Countermeasures primary focus areas and their integration with CI. The primary areas included system studies and risk assessments to create decisional aids, defining threat characteristics and forensics with a concentration on food and agricultural attacks, and surveillance and detection, highlighting interdependencies with the Food and Agricultural Infrastructures. Additionally, he remarked that the biological countermeasures work depended on CIP R&D to identify CI, its needs, risks, and priorities in order to concentrate its impact and efforts. Furthermore, he stressed that Continuity of Operations is an important field that needs to be addressed.

Dr. Vitko stated that the priorities for protecting the CIs in the event of an incident should be determined by the CIP community in partnership with owners and operators. Additionally, he pointed out that the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate focused on chartering and working with information sharing analysis centers (ISACs) and infrastructure communities.

3.4.2 Dr. Tim Oppelt

Dr. Oppelt discussed the EPA's R&D activities surrounding the protection of the water infrastructure and conducting decontamination research in partnership with key federal agencies such as DHS, DoD, HHS, and others. He shared that distribution and water system protection were part of the EPA's cross-agency federal efforts, which require coordinating diverse stakeholders and working with a research consortium in order avoid redundancies and to keep focused. Dr. Oppelt pointed out that the EPA has also demonstrated the positive effects of collaborating with non-federal entities through its relationships with the water and building industries as well as the emergency responder community by collaborating with them on their peer reviews panels, round table discussions, and training and testing.

The EPA focus areas that overlapped with the NCIP R&D Plan's nine themes included:

- Detection and Sensor Systems through surface and water sampling/analysis methods and early warning systems evaluation;
- Analysis and Decision Support Systems through threat scenario assessment and simulation and risk assessment data, methods and tools for modeling/simulation;
- Protection and Prevention through building protection guidance, air filter effectiveness evaluation, and water facility protection/design guidance; and
- Response, Recovery, and Reconstitution through decontamination methods and guidance for structures, water systems, outdoor and systems engineering studies/response playbooks.

Additionally, Dr. Oppelt stated that the EPA was working in other areas that are not accounted for in the themes.

3.4.3 Dr. S. Randolph Long

Dr. Long presented the status of various projects underway for DHS Chemical Countermeasures that related to the protection of CI and he encouraged participants to seek out opportunities to collaborate and enhance each other's work. The DHS Chemical Countermeasures portfolio concentrates on efforts to identify priorities, gaps and overlaps in existing R&D programs, to define the Nation's operational vulnerabilities and gaps in responding to a chemical terrorist attack, and to contribute to an interagency report that shapes the strategy and provides guidance for WMD research and development. Activities related to chemical countermeasures and infrastructure protection included:

- Networked chemical detection systems against broad spectrum vapor threats for buildings and facilities
- Active threat mitigation measures for buildings
- Technologies to determine extent of contamination
- Facility decontamination
- Guidelines to improve infrastructure preparedness

Dr. Long also presented some insights into the areas where he felt more focus needed to be directed. These included the need for better analysis capabilities, detecting emerging threats, creating more agreements among established laboratory networks, and creating forums to coordinate investments.

3.4.4 Mr. Brooke Buddemeier

Mr. Buddemeier spoke about the efforts within the EP&R portfolio and their relationship to CIP. The EP&R portfolio is focused on the implementation of HSPD-8 through a two-pronged approach: bottom-up and top-down. EP&R focuses on integrating new technology to best serve the first responders, creating models and scenarios for events, offering simulation-based training and education, and providing scientific support and technology to enable execution of the National Preparedness Goal. This agency effort is committed to providing the scientific underpinnings and ensuring that new technology fits with the operational end-users' needs.

Mr. Buddemeier recognized that the ultimate implementation of new R&D efforts will require the support and cooperation of members from the emergency services sector. EP&R priorities interconnect with CIP through its support of deploying sustainable technologies to state and local communities that integrate with legacy systems, its work to identify and understand CI "nodes" and vulnerabilities, and its efforts for pre-planning and preparedness to mitigate consequences.

3.4.5 Dr. Laurie Waters

Dr. Waters described the main focus areas of the DHS Radiological/Nuclear (Rad/Nuc) Countermeasures portfolio and discussed links with various themes from the NCIP R&D Plan. The primary Rad/Nuc focus areas protect and prevent against threats from nuclear weapons (stolen or manufactured), radiological dispersal devices, contamination of food and water, and attack on nuclear facilities.

Specifically to protecting CI, Rad/Nuc Countermeasures has recognized that there are interrelated efforts with other agencies and has established memoranda of understanding to jointly support and manage them and has sought to facilitate Rad/Nuc CI protection, prevention, and threat assessments with other agencies. The following Rad/Nuc strategic objectives have a CI-related goal:

- Systems Analysis & Pilot Deployments – Develop supporting information and analysis required to efficiently deploy Rad/Nuc countermeasure systems that improve the U.S. capability to address threats.
- Detection Technology Initiatives – Perform the underlying R&D to develop new or enhanced technologies for the detection of nuclear and radiological materials.
- Preplanned Product Improvements (P3I) – Rapidly develop and transition enhanced capability to currently deployed detectors/systems and rapidly incorporate prototype technologies into commercial offerings for use in DHS operational environments.
- Incident Management & Recovery – Develop new or enhanced capabilities in the areas of crisis response, consequence management and recovery, and attribution.

4.0 MAPPING OF NCIP R&D PLAN THEMES AND GOALS

Every year the federal government spends billions of dollars on R&D projects across a wide spectrum. It is a significant challenge to get an accurate picture of what kinds of R&D projects are being funded, especially in a diffused area such as CIP. The intent of the mapping exercise was to tap into the collective knowledge of the workshop participants to begin to understand where dollars are being spent across the federal government related to CIP R&D and specifically how current resources support the nine themes and strategic goals outlined in the 2004 NCIP R&D Plan.

4.1 Themes and Strategic Goals

During lunch, participants were asked to take some time and map the key projects or programs. The themes and strategic goals were displayed on large "wall art" posters (Figures 3 and 4) in the conference room to facilitate the interactive exercise. There was also an area titled "other" where participants could note projects or programs that did not appropriately align with a theme or strategic goal. As the participants placed notes with relevant project information and points of contact on the posters, the display became a powerful visual that documented where energy and efforts were concentrated, where certain themes were being addressed across Agencies and departments, and which themes needed more investment in terms of energy and efforts. Data from the participants collected on the theme and strategic goals wall art is document in Appendix C.

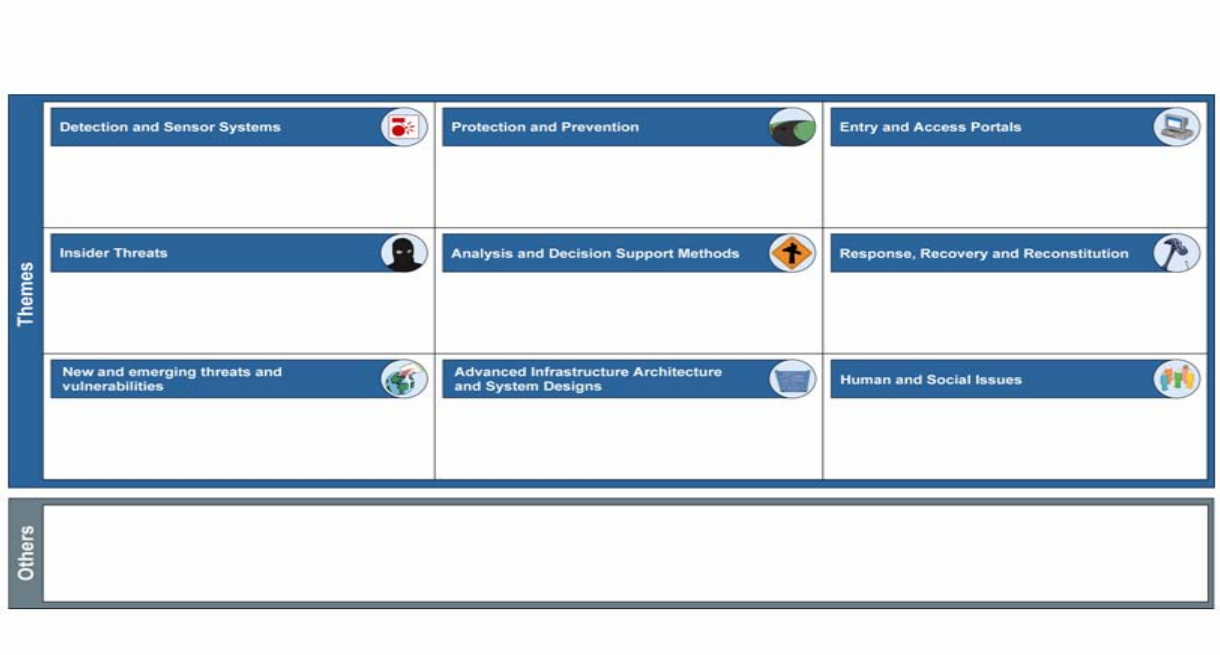

Figure 4 - Wall Art of NCIP R&D Plan Themes

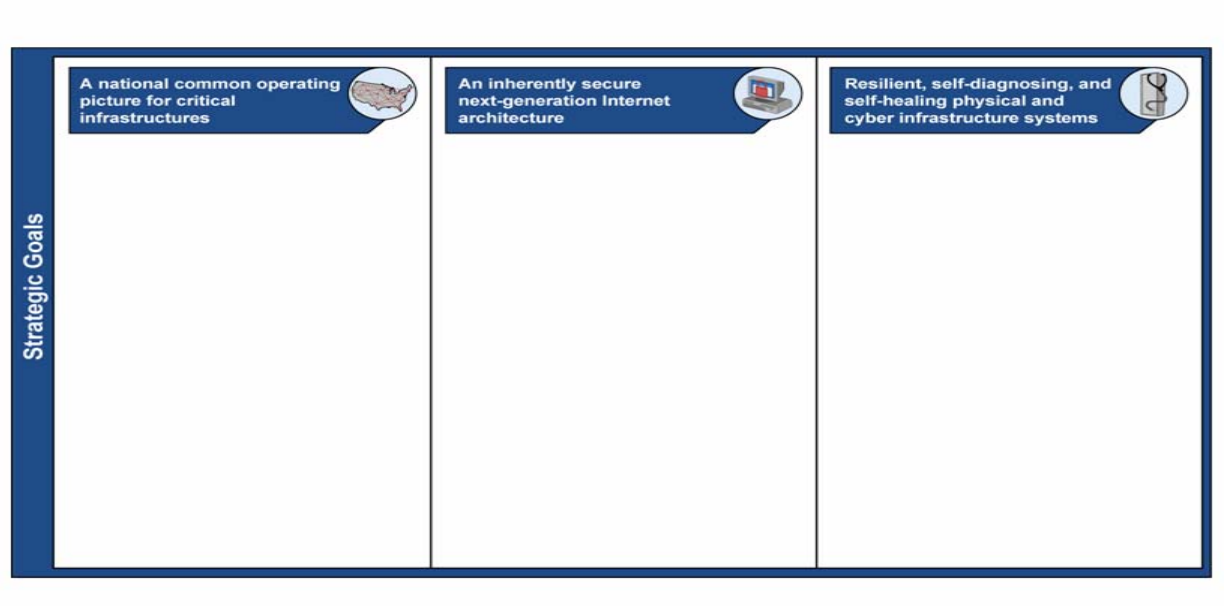

Figure 5 - Wall Art of NCIP R&D Plan Strategic Goals

Once participants had an opportunity to populate the wall charts they were invited to review the display (Figure 5 – if we include a photo) and offered their reflections on what they saw as well as describing efforts in their own agency. As a result, many of the participants were inspired to connect with colleagues from other agencies who shared similar missions to share insights from their current research and development efforts. Refer to Table 1 for the comments captured from the discussion.

Agency	Comments From Representative

NSF	• Cyber trust program
	  o $30 Million dollar budget
	  o Wants research to be relevant
	  ▪ Recognizes that infrastructure is increasingly dependent on cyber
	  ▪ Advanced architecture design
	  ▪ Distinguishing between research and development
	• Who else in the audience cares about these projects?
	  o 7 people raised their hands

	• Portfolio supports all of the 9 themes in the Plan
	  o Open to partnering and building relationships
	  o Works through peer reviews so difficult to prioritize
	  o Open to supporting all research

NIST	• Working in response to the events of 9/11
	  o Looking for partners in building safety – buildings and structures
	  o Objective is to understand how buildings of all types perform during terrorist attacks

Agency	Comments From Representative
	• Focuses on measurement, measurement techniques, & standards o Ready to help o We focus on Metrology: The science of measurement o Involved with NMI - National Measurement Institute o Many instruments require recalibration that NIST can help with o Who else is measuring something? ▪ ***9 participants***
DHS	• Participant recognized the need to normalize risk and vulnerability assessments and measurements • Who else can help? o ***11 participants offered to help***
USACE	• Interested in protecting civil works infrastructures o Protecting dams and preventing them from being Weapons of Mass Destruction o Emphasis on social research ▪ Developed a risk assessment methodology to be used across sectors ▪ Dam Failure Economic study - primary and secondary consequences o Looking to partner with FEMA
Treasury	• Don't have R&D specific projects, but have an R&D agenda and would like to partner o No direct budget; however, its 30,000 institutions can offer possible test bed o Who else shares this interest? ▪ ***2 participants raised their hands***
EPA	• Interested in addressing/protecting water systems o Who can help? ▪ ***7 folks***
USDA	• Focusing on animal, plant, food issues o Wants to have more input with partners on: ▪ Insider issues ▪ Analysis and Decision Support ▪ Entry ▪ Response, recovery, reconstitution ▪ Human and social issues - attacking the human pop. weighs heavily on the psychological mindset of society
DOE	• Addressing the national laboratories o Lab coordinating council is building a database of what their capabilities are and what projects they're working on o Central repository of projects being conducted for CIP R&D o Will look into adding this communities' projects into the DOE database

Agency	Comments From Representative
DoD	• Has programs that help with any/all of the themes o How can DoD help? ▪ There is a CIP integration group ▪ Working to reform and is interested in participating

Table 1 - Agency Comments

5.0 PRIORITIES

Immediately following the mapping exercises, the group participated in a series of exercises designed to come to a consensus (Figure 3) on a set of priority program areas for CIP R&D moving forward. Participants agreed that for workshop purposes, the definition of priority program area was "all areas that will result in a significant new capability for CIP in the next few years."

Federal R&D leaders were invited to participate in this process to illustrate the challenge of identifying and prioritizing CIP R&D requirements and also to begin the difficult task of outlining priority program areas for the 2005 NCIP R&D Plan. In addition, these drills allowed stakeholders to understand alignment and/or gaps to priorities outlined in the 2004 National CIP R&D Plan.

5.1 Agency Priorities

In the first drill, participants were grouped by agency and asked to come up with their agency's top three priorities for CIP R&D; there were no restrictions on the priorities except that they had to align with the previously agreed upon definition of priority program area. Participants were encouraged to utilize "little hat thinking" (Figure 2) while deciding on the top three priorities for their agency. After reaching consensus, each table filled out a template for the group and then one for each person that they took with them to the next drill. The agency priorities are listed in Table 2.

Agency	Agency Priorities
NIST (DOC)	• First responder network tools. Integrated tools for emergency responder network and decision makers that incorporate high fidelity models, validation, simulations and real time data acquisition. • Cyber security, integrated biometrics, authentication, for control systems/SCADA security. • Advanced models, measurements, materials, and test methods in protecting CI.
DHS	• Risk and vulnerability assessment framework o Policies o Tools o Methods o Captures interdependencies (1st order and nth order) • Information synthesis, sharing and integration into a common operating picture. • Develop measures to prevent major disruptions of the internet and electric grid

Agency	Agency Priorities
NSF	• Maintaining fundamental science and engineering research related to CIP • Bridging physical and cyber infrastructure
DOI/ Reclamations	• Analysis and decision support. DOI assets and icons: water, energy. Vulnerability. • Protection and prevention. DOI assets and icons: water, energy. Hardening. Water side strategy. • Human and social special events. Interconnection with critical infrastructure. Cascade consequence(s).
DOT	• Hardening of assets • Sensors and detection. • Emergency transportation operations.
Treasury	• Threats possessed by insiders. • Data replication technology over long distance. • Securing computer off the shelf (COTS) programs.
USDA	• Protection and prevention: bulk detection and inactivation of threats to the food supply (including animals, plants, and food) field deployable. • Human and social – including communication, restoring confidence, research on messages to allay panic, background threats – insider threats. • Protection and prevention; better notification, of agricultural contraband and interdiction at ports - hold and transport control.
DoD/CIA	• Global emerging technologies based on intellectual capital. • Interdependency sector models. • Identifying vulnerabilities and risk based on strategic impact.
FDA/FSAN	• Prevention/Detection of select agents in food: rapid, easy to use, cheap multiple analyses, in line real time. • Agent characteristics in food: steps to destroy agents, processing tools, filters, affinity removal tools. • Dose response – how much agent in a food does it take to cause illness or death?
DOE	• Situational awareness • Criticality and interdependencies • Robust Systems
NASA	• Cybersecurity – attack detection vulnerabilities patching, secure application development • Orbital and sub-orbital detection and hacking of technological and environmental hazards. • Aviation safety and security through research in aircraft systems hardening and securing of air space operations.
EPA	• Sensors and analytical technique for real time detection of NBC agents. • Early warning of intrusion, analysis (lab capacity), public health surveillance, security.

Agency	Agency Priorities
	• Decontamination, response, recovery, reconstitution
DOJ	• Cybersecurity and the interface between other agencies • Analysis and decision support methods: tie nationally critical functions/services to mission critical IT systems. • Detection systems as they apply to IT systems. This also includes awareness of new and emerging threats and vulnerabilities.

Table 2 - Agency Priorities

5.2 Interagency Priorities

After leaving their Agency groups, participants were asked to move to interagency tables comprised of members from different agencies. These table configurations were "designed" for maximum diversity of agency representatives and perspectives. With their already agreed upon agency priorities in hand, participants had a dialogue to come to a consensus at their interagency tables on the top 3-5 priorities for the Nation in CIP R&D. Instead of wearing the "little hat", participants were asked to put on their "big hat" and take a broader view of the Nation's anticipated CIP R&D priorities. Table 3 contains the results of the interagency priority exercise. Note: some interagency tables combined to ensure maximum participants at each table and therefore some table numbers are missing from Table 3 below.

The various backgrounds and perspectives represented at the interagency tables proved valuable to the participants as they had an opportunity to not only learn where other agencies where focused but also what R&D their colleagues thought was most important to protect the homeland.

Interagency Table	Interagency Table Priorities
3	• Maintaining the Nation's technological edge in basic sciences & engineering • Resilient self-healing, self-diagnosing, adaptive, damage-limiting, physical, biological & cyber infrastructure systems • Risk and vulnerability assessment framework supporting policies, tools (including models and simulation), methods, standards & measurements that capture 1st and nth order interdependencies and support near- and long-term exercises • Information synthesis, sharing and integration into a common operating picture and structure • Sensors and detection technologies that are inexpensive, reliable, field deployable and interoperable

Interagency Table	Interagency Table Priorities
4	• Protect and prevent: (merge with insider threat) o Agriculture o Germ plasm o Cyber and physical security o Vaccines o Hold and transport sampling • Detect and Sense: o NBIS • Analysis and Decision: o Risk Assessment • Response, Recovery and Reconstitution: • Human and Social Issues: (merge with insider threat)
5	• Situational Awareness and Rapid Response o Develop a COP System that rapidly identifies existing and emerging threats and vulnerability and proper analysis and strategically focused response • System capability to identify and prioritize key resources and capabilities – based on a standardized enterprise (access and information) architecture • Government standards and policies incorporating cyber security with authentication and biometrics for control based on enterprise (national architecture) • Comprehension and understanding of infrastructure
6	• Identification and Monitoring of CI vulnerabilities to potential emerging threats and compare to groups that have access to such threats o Links to Emerging threats and vulnerabilities • Development of risk and vulnerability assessment framework, including tools, materials, and policies o Links to Analysis and Decision Support Methods • Conduct research into means of detecting and manning the risk of Insider Threats • Expand research into improved response related to human and social aspects resulting from an incident • Information synthesis, sharing, and integration into a common operating structure/picture
7	• Prevention through detection: Detection and Systems • Analysis and Decision Support for Instant Response and Recovery • Maintaining of fundamental research • Human technology and social interface • Bridging the Cyber and Physical Infrastructure
8	• Risk Assessments and Vulnerabilities will drive investments • Cyber Security

Interagency Table	Interagency Table Priorities
	• Response & Recovery: o Integrated tools for first responders, containment, decontamination • Detection Systems • Information synthesis, modeling, measurements, and synthesis
9	• Cyber/SCADA • Continuous Forecasting for Technology Innovation • Response/Recovery/Restoration • Geospatial Technologies Integration with Sensors • Interdependencies
11	• Fundamental research in science and engineering fundamental models, measurements, and materials • Situational awareness sensors, detection, and data mining • Robust systems with cyber security, safe communications, and hardening of assets • Human and Social Issues: Adapting to change and work force issues

Table 3 - Interagency Priorities

5.3 National "Presidential" Priorities

After reaching consensus at their tables and filling out the "Interagency template", the entire group was led through a facilitated session intended to come up with the top 5- 7 priorities for the nation. Participants volunteered their perspectives on what priorities should populate the final list and eventually, through continually accepting, rejecting, and justifying every priority that was suggested, a consensus list was developed and is provided below in Table 3. It is interesting to note that this priority list closely aligns to priorities defined in the 2004 NCIP R&D Plan.

Priority Program Areas for CIP R&D Per Workshop Participants

1: Resilient, self-healing, self-diagnosing, adaptive, damage limiting, physical, biological and cyber human infrastructure systems
• Sensors and Detections Technologies that are inexpensive, reliable, field deployable, interoperable, and secure
• Cyber Security (includes biometrics, authentication, controls systems/SCADA security) based on Enterprise/National Architecture
  o Including integral security in systems
  ▪ Looking at future systems as you build

2: National Common Operating Picture • Sector interdependency models that lead to priorities situational awareness communication within Common Operating Picture (COP) • Rapidly Identifies Existing and Emerging Threats and Vulnerabilities • Properly analyzes and executes a strategically focused response • Integrated tools for first responders and decision makers that incorporate high fidelity

Priority Program Areas for CIP R&D Per Workshop Participants
models and real time data acquisition • Vulnerability and Risk Assessment in a Dynamic Environment (Full lifecycle: tools, requirements, methods, standards…) o Must drive the investment for all other priorities and right now we're not sure how that will happen o Cyber and physical and human elements ▪ Attacks across all sectors
3: Secure National Communication Network
4: Technology monitoring and forecasting intellectual capital the movement of technology
5: Human and Social Issues
6: Access to information about sensitive, complex systems and validation techniques of complex models

Table 4 - National CIP R&D Priorities

5.4 OMB "Mock" Resource Allocation

Finally, interagency tables had an opportunity to "act is if they were OMB" by deciding where federal dollars should be allocated. Each table received 100 poker chips, representing a notional $1 Billion, and a game board where they scribed the previously agreed to priority program areas. Participants were asked, as an interagency table, to allocate the chips according to where they thought money should be spent. Note: there were no restrictions on how the money was to be spent except that they had to spend all 100 chips. This exercise was intended to illustrate the decision making challenge and difficult prioritizing process that OMB must work through every year when deciding how to allocate funds across the federal programs. Figure 5 below illustrates the results of this exercise.

	Priority Budget Calculator						
	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	*Total*
Tables	**Resilient self-healing systems**	**National Common Op. Picture**	**Secure Nat. Com. Net.**	**Tech. monitor & forecasting**	**Human and Social Issues**	**Access to sensitive info.**	
2	18	41	17	7	4	13	100
3	49	13	7	13	17	1	100
4	40	40	10	5	5	0	100
5	30	38	18	2	8	4	100
6	35	35	10	5	15	0	100
7	33	32	8	5	18	4	100
8	37	38	12	3	5	5	100
9	30	30	20	10	5	5	100
11	30	30	0	0	20	20	100
12	30	35	16	11	8	0	100
Total	332	332	118	61	105	52	
Avg	33	33	12	6	11	5	1000
Median	32	35	11	5	8	4	
Mode	30	38	10	5	5	0	
Appx. Std Dev.	8.1	8.1	6.1	4.1	6.3	6.5	

Figure 6 - Program Area Money Allocations by Interagency Tables

Results from the "mock" OMB chip allocation drill highlight the consistency in thinking among the workshop participants as the first three priorities were most heavily budgeted. Interestingly, these three priority program areas were consistent with the priorities laid out in the 2004 NICP R&D Plan, highlighting an alignment between the Plan and the best thinking of the workshop participants.

6.0 CONCLUSION

The beginning of the Federal Leaders Workshop for the CIP R&D began with a resounding endorsement from the agency keynote speakers for the work being undertaken, and re-emphasized the role of CIP R&D in protecting the country. With the "go-ahead" to move forward, the keynote speakers sanctioned the participants to continue their efforts and offered areas of focus for future CIP R&D efforts. The participants were also introduced to the HSPD-7 mandate—the primary reason for coming together—and were encouraged to engage in the process for developing future NCIP R&D Plans. By drafting priorities for the 2005 NCIP R&D Plan and ranking their importance through a budget exercise, the participants established an initial framework for the progress that will be achieved in the coming year.

The Workshop provided an opportunity for the research leaders to kick off new discussions with their colleagues on future CIP R&D planning, needs, and priorities. This was achieved through several group activities that involved varying agency perspectives to show a holistic view of the future for CIP R&D. The participants were strongly encouraged to continue to seek opportunities to collaborate with one another in order to better protect critical infrastructure and build the intellectual relationships with their counterparts in other federal agencies and departments.

In the coming year, the CIP R&D planning team has promised to achieve a new level of depth for the Plan and to set up implementation mechanisms. Goals identified for the 2005 NCIP R&D Plan

include documenting milestones and budgets based on input collected from agencies and partners, ensuring that the voice of industry is woven into the process through workshops, involving academe, and seeking out partnerships with the sector coordinating councils as a mechanism for understanding the owner and operator priorities.

In order to ensure each version of the Plan truly represents the interest of the CIP R&D community, the call to action was placed on the participants of this workshop. They were asked to help identify others who needed to be contacted and incorporated into planning process for the 2005 NCIP R&D Plan.

As the CIP R&D Leaders Workshop came to a close, the enduring message to the participants stressed the importance of following up with the conversations and acquaintances initiated during the workshop as a beginning for new partnership opportunities for the advancement of critical R&D efforts. The end of the day was not the end of these discussions but a launch for planning into 2005.

APPENDIX

Appendix A—High Level Agenda
Appendix B—Question & Answers from Breakout Sessions
Appendix C—Agency Priorities and Interagency Priorities from Afternoon Breakout Session
Appendix D—Participant List

APPENDIX A—HIGH LEVEL AGENDA

Sheraton Crystal City—Washington, DC
December 16th, 2004
7:30am-4:30pm

I. Continental Breakfast and Networking (7:30-8:00 a.m.)

II. Introduction and Objectives

III. Agency Keynotes – Their Perspectives on Homeland Security Research & Development (R&D)
- Dr. John Brighton, Assistant Director for Engineering, National Science Foundation
- Dr. Hratch Semerjian, National Institute of Standards and Technology (NIST)
- Dr. Charles McQueary, Under Secretary for Science and Technology (S&T), Department of Homeland Security (DHS)
- Dr. John Marburger, Director, Office of Science and Technology Policy (OSTP)

IV. Overview of Homeland Security Presidential Directive-7 (HSPD-7)

V. Overview of 2004 National Critical Infrastructure Protection (CIP) R&D Plan and other CIP R&D Related Plans

VI. Break

VII. Panel-- DHS/S&T Portfolio Managers and other agency representatives to discuss the various "links" to CIP; including chemical, biological, radiological, nuclear, and Emergency Preparedness & Response (EP&R)
- Dr. John Vitko, DHS Biological Countermeasures
- Dr. Tim Oppelt, Environmental Protection Agency (EPA) Biological and Chemical Countermeasures
- Dr. Randy Long, DHS Chemical Countermeasures
- Mr. Brooke Buddemeier, DHS EP&R
- Dr. Laurie Waters, DHS Radiological and Nuclear Countermeasures

VIII. Networking Lunch (will be provided)

IX. First Glimpse of 2005 CIP R&D Priorities

X. Open Discussion

XI. Closing Remarks

APPENDIX B—QUESTIONS & ANSWERS FROM BREAKOUT

1. *What is and isn't Critical Infrastructure?*
    a. From the Homeland Security Act and HSPD-7, critical infrastructures are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. This includes everything from water and food infrastructures, to transportation, finance, and a dozen other areas, including the ubiquitous cyber security and information network infrastructure. What is not CI requires a more flexible definition based on a specific infrastructure and its components. For example, CIP does not have responsibility to develop the sensor technologies for detecting malevolent biological agents in our water, food, air environments – rather, CIP is responsible for the deployment and integration of these new technologies in a manner that maximizes their effectiveness while remaining interoperable with larger or adjunct systems.

2. *When does industry, including owner and operator and the industry that supplies them, start coming into the 2005 CIP R&D?*
    a. An industry workshop with the R&D representatives is planned for February or Spring 2005.
    b. DHS is partnering with the Sector Coordinating Councils and the Information Sharing and Analysis Centers (ISAC)5
    c. First, we need the have the 2004 NCIP R&D Plan signed and in the public domain
    d. In 2005, the National Plan will include a R&D roadmap that will coordinate with private industry, specifically on issues related to commercialization

3. *Do the themes in the NCIP R&D Plan cover what the group (Federal Government) is doing? Is there a prioritization of themes and priorities? How are we going to focus the topics in Plan?*
    a. The 2004 NCIP R&D Plan was developed by members (and other designees) of the ISC of the NSTC. The ISC membership includes 23 Federal agencies, most of which are participating in this workshop. In general, the 2004 NCIP R&D Plan is representative of the R&D work performed in the Federal agencies, but is not necessarily complete. The selection of the themes and prioritization of the main objectives represent the best efforts of the ISC working these issues over the last year. One of the goals of this workshop is to vet the themes and priorities, adjusting each as appropriate prior to developing the 2005 National NCIP R&D Plan. We anticipate, based on a broader range of stakeholder input, that the 2005 Plan will be more focused and better aligned with national priorities in CIP.

[5] The Sector Coordinating Councils are policy-level organizations charged with representing a sector strategy for addressing infrastructure protection. They work with Government Coordinating Councils to identify needed initiatives and timelines for implementation - and usually work with ISACs to disseminate information on the latest homeland security issues, like terror threats.

4. *Is there a plan to bridge the physical and cyber research in the roadmap? How do cyber and physical themes get tied together?*
    a. A central tenet to the National CIP R&D Plan is to ensure that physical and cyber R&D efforts represent an integrated effort. While there may exist elements in each R&D agenda that may be developed independently, the pervasive nature of the cyber component suggests that the impact with the physical is significant and must be included in the early phases of development.

5. *Clarification on "Industry": Do we mean the Owners & Operators or Vendors (those providing services to this segment of the market).*
    a. We include both groups in this category. Primarily, we look to the owners and operators, in partnership with the Federal government, to define the capabilities and gaps in our current technologies. Technologies vendors partner with the Federal research communities to identify and develop new and innovative tools needed to protect our critical infrastructures.

6. *Is there a collaborative process to CIP R&D?*
    a. The National Science and Technology Council is the primary partnering vehicle for the Federal agencies. Collaboration with academia and the private sector will follow through a variety of venues including workshops, grant competitions, and non-governmental entities such as the Sector Coordinating Councils.

7. *How do we minimize redundancy?*
    a. Effective collaboration is the primary tool that will limit redundancy in the Federal R&D CIP research and development agenda. See 2a above.

8. *What is the game plan? How do we get agencies to work together?*
    a. One of the fundamental challenges in Homeland Security environment is to develop better federal agency cooperation. Key to addressing this challenge is a mutual understanding of the goals, objectives, and as importantly, the challenges in their implementation. With federal agencies facing increasingly tight budgets, better collaboration, partnering and leveraging resources are required. In the 2006 budget cycle, OMB will have a separate line item in the President's budget representing the Federal agency programs in homeland security and infrastructure protection and will provide a first definitive step toward better planning and execution.

9. *Who are the customers of the NCIP R&D Plan?*
    a. The primary customers are the owners and operators of the nation's CI[6]. The stakeholder community for CIP is much larger: the Federal, state and local governments also have responsibility to protect government operations, the economy, and the American people from the effects of failures to our infrastructures. The vendor community represents a customer base in making available effective commercial products and technologies to protect CI across a broad range of applications.

[6] It is estimated the 85% of the critical infrastructure is in the private sector

10. *How does the Matrix Project fit into the scheme?*
    a. The Matrix Project is one aspect of the current efforts in the federal sector to protecting critical assets and facilities
    b. It's a tool to understand issues of asset identification and consequences of attack.

11. *What is the relationship of the R&D Plan and implementation for CIP - intelligence and countermeasures?*
    a. The NCIP R&D Plan needs strong linkages to a number of other plans and planning efforts. The Intelligence community and WMD (Chem, Bio, Radiological, and Nuclear) countermeasures are two important groups.

12. *How does the NCIP R&D Plan influence investments outside of R&D? Will the budget process be affected by the roadmap?*
    a. The National Infrastructure Protection Plan (NIPP) is mandated by HSPD-7 to identify, prioritize, and coordinate the protection of CI and key resources in their respective sectors. The implementation of the NIPP will be influenced by the goals, objectives, and technology roadmap developed in the NCIP R&D Plan.
    b. Beginning FY05, OMB will have all Federal homeland security R&D investments as a separate line item in the budget. This will facilitate the coordination of CIP R&D investments across the Federal government.

13. *How can we resolve the divide on threat assessments between professionals and the intelligence community?*
    a. There are different communities and different cultures with different understandings and perspectives. Developing a mechanism to share information and cooperate to protect the nation's CI must be identified and developed and unfortunately may be beyond the scope of this effort.
    b. There is a need to establish common definitions, terminology and ontologies so that the two communities can establish a dialog and begin to share appropriate information in a secure protect manner.

14. *How are we going to understand things in the broader area that are not apparent?*
    a. Incorporating input from multiple stakeholder groups including industry, the intelligence community, and Department of Defense (DoD) in both formal public settings and individually will aid our effort in understanding the scope and breadth of the challenges to protecting CI. While elements of this dialog may not be made public for confidentiality or sensitivity concerns, they can help guide the general direction and objectives to the National CIP R&D Plan.

15. *How do you spur basic research to the CIP objectives?*
    a. While basic research is the providence of both the Federal and private sector, traditionally for areas of broad application or long-term/deferred payback, the Federal R&D enterprise often takes the lead role. Federal funding for CIP R&D requires a strong, well-organized research and development plan. The NCIP R&D Plan is precisely the vehicle that Congress and OMB intended to provide such direction and coordination.

16. *How do you include biological research?*
    a. Biological R&D will be covered in the Bio Countermeasures R&D Plan.

17. *Given the extensiveness of its research, how do we incorporate DoD?*
    a. The Department of Defense has been an active member of the ISC for the past year.

18. *How do you factor economics into environmental risk?*
    a. The ongoing work on risk analysis by ASME (RAMCAP Project) and others provides a rigorous foundation to the subsequent economic analysis of viable alternatives. Assessing economic benefit relative to multiple objectives such as life-cycle costs, environmental impacts, and similar measures is an area of active development within the public and private R&D community (see for example, Chapman (NIST, 2004).

19. *How do we assess the psychological issues that result from an attack or disasters?*
    a. The social and behavioral issue is an important area of future research. This issue is the focus of one of the nine major themes in the 2004 National CIP R&D Plan. Admittedly, this theme and the development of an appropriate research agenda must be significantly advanced in the coming years. We will look to NSF and other agencies for continued support in the developing the analytical basis for social and behavioral issues related to catastrophic events and to homeland security in general.

20. *How will CIP results be shared?*
    a. We expect that the 2004 National CIP R&D Plan will be publicly available in February 2005. In the Spring, a workshop with industry representatives will use the results from the plan and this workshop as a basis for their discussions. Similarly, a future workshop is envisioned focused on researchers from academe, national laboratories, and the broader R&D and homeland security communities.

21. *How do HSPDs 7, 9, 10, & 11 relate to each other?*
    a. Cyber and Physical are interlocked in the plan
        i. They are in the plan as Interlinking puzzle pieces in the puzzle.
    b. HSPD 9 establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
    c. HSPD 10 "BioDefense for the 21st Century " is a classified directive that establishes a national policy along the lines of the Biowatch program.
    d. HSPD 11 is responsible to i) enhance terrorist-related screening through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to

homeland security and to ii) implement a coordinated and comprehensive approach to terrorist-related screening.

22. *How does this relate to HSPD 11?*
    a. See question 21 above.

23. *What role can a largely R&D consumer play in this workshop?*
    a. Participate actively and help define needs, requirements, and gaps that science and technology can fill.

24. *How will HSPD 9 & HSPD10 get integrated?*
    a. HSPD 9 establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
    b. HSPD - 10 BioDefense for the 21st Century
        i. Overall bio defense

25. *What is considered the Critical Infrastructure in Agriculture & Food?*
    a. The "system" that starts on the farm and ends with meals on the tables has numerous critical and key nodes and assets.

Questions from the Panelist Discussion

26. *Is this group addressing emerging threats (such as electromagnetic threats)?*
    a. It is part of the plan and an overall theme
    b. There is not a specific working group right now

27. *What are the legal implications of identifying CI that have low frequency, high probability, and high impact of attack?*
    a. Information sharing is difficult
        i. As work progresses and research is deployed, basic information can be shared with the community.
        ii. The National Asset Database is kept secured - not shared with the public
    b. Cities often share guidance and needs with the Federal Government

28. *What are the priorities for protecting the CIs in the event of an incident?*
    a. Resources that need to be protected should be prioritized by the CIP community
    b. We partner with the owners and operators
        i. e.g., IAIP is focused on working with the Sector Coordinating Councils, the ISACs and infrastructure communities

APPENDIX C—AGENCY PRIORITIES AND INTERAGENCY PRIORITIES

C-1 Themes:

Themes	Agency	Project	Point of Contact
1.1 Detection and Sensor Systems	NSF	NSF Sensor and sensor networks: designs, materials and concepts for new sensors and sensing systems, arrayed sensors networks and networking research and utilization of sensor data.	Fil Bartoli ECS/NSF
		NSF Engineering Research Center: • Large centers ~$3 Million/year. Topics include: sensing and storms and atmospheric hazards, sensing and imaging, wireless devices.	Lynn Preston
		NSF/MPS • Sensors • Sensor manufacturing • Sensor management – communication • Motion tracking • Intrusion detection	Unknown
		NSF/MPS - Sensor Technologies: • Next generation devices • Detectors of toxic agents • Sensor arrays • Sensor assessment of reliability, and validation	
		NSF/MPS - Imaging and pattern recognition.	
		NSF/MPS - Development of nanostructures, materials technologies for sensors and detectors	

Themes	Agency	Project	Point of Contact
		NSF/MPS – Support the development of materials in infrastructure systems	
		NSF/MPS – Development of sensitive selective analytical techniques for chemical and biological agents	
	NIST	Sensor Performance Evaluation Standards	William Grosshandler (301) 975-2310
		RFID chips – security – passports, etc…Security to prevent alteration.	Carol Handwerker Carol.handwerker@nist.gov (301) 975-6158
		High Energy – Active Interrogation: Performance and safety standards, technology, validation.	Lisa Karam (301) 975-5561
		Rad/Nuc Detection: Standards, interoperability, T&E protocols.	
		High Sensitivity, low cost sensors for HS applications: Development of a new generation of ultra-high sensitivity sensors for perimeter control, imaging, etc…	Dennis Friday (303) 497-3121/3131
		RF and Microwave Electromagnetics (EM) R&D related to wireless propagation, sensing and imaging; EM weapons detection characterization and vulnerability assessment	
		Chemical Reference Materials for Trace Explosives: • Reference materials • Performance guidelines	J. Greg Gillen (301) 975-2190
		Sensor network standards (interoperability)	Al Wavering wavering@nist.gov
	DHS/TSA	Fusion of existing radar data (ie. FAA ground radar, USCG radar) for perimeter intrusion detection	Mark Torbeck

Themes	Agency	Project	Point of Contact
		Biometrics standards development and improved performance research	Rick Lazarick
		Development of bulk sensors for explosives and weapons detection (physical – i.e, X-ray, CT, etc.)	Dr. Ron Krauss
		Development of Trace Sensors for Explosives Detection	Dr. Richard Lareau
	DHS	Cyber Security Portfolio, Next Generation Cyber Security Technologies Program, topic areas: • Vulnerability detection, protection mitigation identity theft protection, trustworthy infrastructure	Simon Szykman Simon.szykman@dhs.gov
		Cyber Security Portfolio, Internet Infrastructure Security Program	Simon Szykman Simon.szykman@dhs.gov
		Improved CCTV and multi-sensor systems for automated understanding	Peter Miller DHS S&T Program Manager
	USDA	Ag R&D/Grain Tracing/Tracking (CSREES)	Kitty Cardwell
		Food emergency response network	Patrick McCaskey Patrick.mccaskey@fsis.usda.gov 706-546-3314
		Detection. National Animal Health Lab Networks. CSREES (Bill Wagner). APHIS (Larry Granger). Early detection, surveillance of animal diseases. Response to outbreaks (surge capacity).	Bill Wagner wwagner@csrees.usda.gov Larry Granger Larry.m.granger@aphis.usda.gov
	DOE	Real time grid reliability management. Objective: create a robust, available, synchronized data measurement infrastructure of the eastern interconnection for better planning, operational reliability and security	Phil Overholt 202-586-8110

Themes	Agency	Project	Point of Contact
		Basic Research with possible dual-use for CIP: • Materials • Sensors: chemical, rad/nuc, bio • Analytical chemical • Nanoscience and technology	John Miller Office of Science Basic Energy Sciences
		Advanced Sensor Monitoring System for Refinery Applications. Refinery Awareness Security System. Wireless Sensor Network for Energy Asset Protection (anticipating theory – architecture). • National Lab CIP Database of capabilities, emerging technologies	Hank Kenchington 202-586-1878 Mike Soboroff 202-586-4936
	DOT/FTA	Early warning crisis management system for the WMD attacks within the subway	Rhonda Crawley
		Automated Airborne Flight Alert System (AAFAS)	James Rogers
	DOT/FHWA	State of the art bridge surveillance and security techniques	Sheila Duwadi
	DoD/NSWC	Vapor, liquid, solid tracking – B Dep't (NSWC Dahlgren)	Dale Sisson
		Bio-chem detection and sensor systems – B Dep't (NSWC Dahlgren)	
	DoD/OSD	?	Dr. Howard Marsh
		Sensors and Electronics	Dr. John Studstad
	DoD	Counterterrorism Technology Task Force	Bill Riley
	NSA	Sensor Research	Dr. Cliff Hill
	U.S. Army Corps of Engineers	Regional Monitoring	Dr. Will McMahon
		Detection of Waterborne Attack	Dr. Will McMahon (ERDC)
	NASA	Protect Asset Flight System (PAFS)	Susan Wilz
		Detection and Sensors: • UAVs (surveillance)	Terri Goodwin 650-604-1700

Themes	Agency	Project	Point of Contact
		• Cyber/harden aviation network • Chem/bio sensor (airplane cabin air detector) • Security incident reporting mechanism • Data mining (ie. cargo screening) • Biometrics	
	FDA	New methods for detection of threat agents in food for micro, chem., and rad.	David Acheson
	EPA	• Sensor evaluation (CBR) • Sensor testing (ETV) (CBR) For drinking water and wastewater systems	Jon Herrman

Themes	Agency	Project	Point of Contact
1.2 Protection and Prevention	DHS/FEMA	Risk management series: FEMA Guidance Publications: ongoing program to develop guidance for design professionals and decision makers using state of the art physical security knowledge/technology (in coordination with numerous government agencies and private sector groups) (Developed with modest budgets)	Unknown
	DHS	Cyber security portfolio. Cyber Security SBIR Program. Topics: • Cross domain network attack correlation • Real time malicious code detection	Simon Szykman Simon.szykman@dhs.gov
		Cyber Security portfolio. Next Generation cyber security technologies program. Topic areas: Wireless security.	
		Process control systems forum. Next generation process control and SCADA secure architecture	Peter Miller DHS S&T Program Manager
		Improved distributed process control and SCADA security (SBIR Phase II)	
	DHS/TSA	RFID Technology demonstrations • Standards development • Vehicle/baggage/cargo/container tracking	Buzz Cerino
	DOT/FMC	Expanded satellite based mobile communications tracking (Pilot	Dawn Tucker

Themes	Agency	Project	Point of Contact
	SA	Test)	
		Untethered trailer tracking system (Pilot Test)	
		HAZMAT operational test	Joe DeLorenzo
	DOT/RSPA	Toxic Inhalation Hazards (TIH)	Fritz Wybenga
	NSF	Structural systems and engineering: high performance materials, dynamic loads in structures (blast, earthquake, wind) safety/reliability of infrastructures; rapid response assistance	Steve McCabe
		Geotechnical and geohazards systems: geohazards mitigation (earthquake, tsunami, landslide); remediation/containment of geo-environmental contamination soil dynamic and blast response of geologic materials, rapid response reconnaissance.	Richard Fragaszy
		Cyber trust and Sol Greenspan. Wide range of research on protection/prevention (and tolerance) of cyber systems attacks.	Carl Landwehr
	USDA	Ag R&D diagnostics. Infrastructure national diagnostic lab networks. CREES	Kitty Cardwell
		R&D on diagnostic methods, pathogen-host interactions, vaccine development for prevention. USDA-CREES- Peter Johnson. USDA-ARS – Joe Spence.	Peter Johnson pjohnston@crees.udsa.gov 202-401-1896 Joe Spence jcs@ars.usda.govs
		Methods development: detection of threat agents in food matrices.	Lynda Kelley Lynda.kelley@fsis.usda.gov 706-546-3314
	NIST	Emergency communications for First Responders: field mapping for dead spots in buildings; communications in collapsed buildings	Kate Remley (303) 497-3652
		Safety of threatened buildings: increased structural integrity; high performance steel and fire resistance materials; improving emergency egress/access; developing building equipment standards and guidelines	William Grosshandler (301) 975-2310
		Soft body armor standards: performance of vest materials and performance of frangible bullets	Carol Handwerker Carol.handwerker@nist.g

Themes	Agency	Project	Point of Contact
			ov
		Jamming and detection of wireless remotely detonated bombs	Dennis Friday (303) 997-3131
		Cyber security- detection technologies for intrusions and for intelligence purposes; cyber security for hardened secure systems for federal non-sensitive systems	Ed Roback
		Pipeline safety- measurements of standards for pipeline materials to access extent of damage on attack, either intentional or unintentional	Carol Handwerker (301) 975-6158
	DoD	Explosive blast modeling	John Wright (NSWC)
		Blast mitigation for civil works infrastructure, dams and locks	Dr. Will McMahon (USACE)
		Bio/ chem. Protection	Dale Sisson (NSWC-Dahlgren)
	FDA	Agent characteristics determine survival of threat agents in food, role of different processing techniques	Dave Acheson
		Prevention of contamination of the food supply. E.g.- tamper proof packaging, threat agent sensors, neutralization techniques	
	NRC	Evaluation of impacts on concrete/ steel structures (impacts including explosives, vehicles, etc.)	Mark Cunningham
	EPA	Apply blast methodologies to drinking water and wastewater facilities. Further development of techniques	Alan Hais
	DOE	• Critical Infrastructure Test Range • Cyber Security for Utilities • Cyber Security Training and Awareness • Cost-effective Assessment Tool to Identify Critical Nodes • Risk Assessment Methodologies for Energy Infrastructure	Hank Kenchington (202) 586-1878 Mike Soboroff (202) 586-4936
	Unknown	Cyber –harden communication networks in aviation systems; biometrics; electromagnetic energy research	Unknown

Themes	Agency	Project	Point of Contact
1.3 Entry and Access Portals	NSF	Authentication for biometrics – evaluation. Efforts at WVU (Hornak/Shackers), (DHS JT Fandy ?), and at JHU/Lehigh/CMU (Monrose)	Carl Landwehr
		IDS/intrusion detection	Unknown
	DOT/OST	Common identification system	Vicki Lord
	DOT/FAA	Adaptive quarantine	Deborah Hermann
	NIST	High sensitivity, low cost sensors for H.S. application: development of a new generation of ultra-high sensitivity sensors for perimeter control, imaging, etc.	Dennis Friday 303-497-3121
		Standards and protocols for biometrics	Marty Hermann Martin.hermann@nist.gov
		Radiological/nuclear: protocols, testing/interoperability standards, evaluation, standards, calibrations.	Lisa Karam 301-975-5561
		High energy x-ray and active interrogation performance and safety standards.	
	DHS/TSA	Transportation Worker Identification Card (TWIC) (Physical and logical access control/smartcard)	Steve Parsons
		Exit lane breach control portals – standards development, RDT&E	Paul Ruwaldt
	DoD/NSWC	Counter drug interdiction/detection model (NITMAC, NSWCDP Dahlgren)	Elizabeth D'Andrea
	USDA	Ag R&D Sampling procedures. Hold/shipping. CREES/APHIS	Kitty Cardwell

Themes	Agency	Project	Point of Contact
1.4 Insider Threats	NSF	• Networking Security • Database management – knowledge mining • Motion tracking	Unknown
		Cyber trust – insider threat in cyber systems – anomaly detection research, forensics research	Carl Landwehr
	DHS	Improved surety for private security guards	Peter Miller DHS S&T Program Manager
		Mitigating insider threat	

	USDA	Being able to conduct background checks on new employees continue to be a challenge to address insider threat. Is there legal research on how that could be facilitated?	P.R. Santiago 202-205-0452
	NSA	Unknown	Daryl Wilson
	ARDA	Unknown	Dick Brackney
	Secret Service	Unknown	Dr. Marissa Reddy

Themes	Agency	Project	Point of Contact
1.5 Analysis and Decision Support Systems	DHS	Fast simulation and modeling of the electric distribution grid for detection and prevention of cascading failures	Peter Miller (S&T)
		Baseline risk assessment methodology for IT sector: Which of the varied models out there works best for IT?	Mike Lombard Mike.lombard@dhs.gov
		Baseline vulnerability assessment methodology for IT sector: which of the varied models out there works best for IT?	
		How to measure (normalize) results from disparate assessment methodologies?	
		CIP Decision Support System: Three National Labs are developing a consequence based interdependency model for all 14 infrastructure sectors	John Hoyt John.hoyt@dhs.gov John Cummings
		Modeling and simulation of impact of security sensor systems on passenger/ baggage/ cargo queueing/ throughput	Diane Wilson (TSA)
		Risk Assessment modeling tool: HAZUS software tool (existing). A loss estimation tool for natural hazards (EQ, flood, and hurricanes) with applicability to man-made hazards thru existing interface capabilities and by linking to other tools thru a GIA platform. Large IT investment over 10 years	FEMA
	DoD	Vulnerability Assessment tools for dams and buildings	Dr. Reed Mosher (USACE)
		Mobile Assessment Suite	John P. Keenan (DPO-MA) Dahlgren
		Defense Critical Infrastructure Program: vulnerability assessment	Bill Bryan (OSDHD)

Themes	Agency	Project	Point of Contact
		management and development; common operating picture; information sharing; decision support; enterprise architecture	
	DOT	NCHRP- methods for determining transportation and economic consequences of terrorist attacks	Dawn Tucker (OST)
		Measuring and visualizing the risk of hazardous materials in urban areas	
	NIST	Modeling and Simulation interoperability/ integration standards	Al Wavering wavering@nist.gov
	NSF	Knowledge mining; natural language; machine language translation	
		Automated analysis/response to cyber attacks	Carl Landwehr
		SBIR - Cyber security; machine translation; energy systems; hyper spectral imaging	
		NSF/ONR partnership in Electric Power Networks Efficiency and Security (EPNES)- efficient and secure power networks under certain demand	Usha Varshney and Kishem Baheh (ECS)
	EPA	Vulnerability Assessment methodologies for drinking water and wastewater facilities; Physical security standards for water facilities	Curt Baranowski
	NASA	Computer models and algorithms, interoperable COP: knowledge discovery tools/ advanced data mining; common operating picture of National airspace with tools to detect real-time rogue aircraft using federal and DoD sensors	Terri Goodwin (650) 604-1700
	NRC	Vulnerability / risk analysis methods for complex scenarios (e.g. Multiple assaults)	Mark Cunningham
	USDA	Aerobiology and remote sensing (multiple projects); Modeling/ forecasting; CSREES	Kitty Cardwell
		Survivability/ viability of threat agents in food matrices	Lynda Kelley
		Inter-regional input –output matrix development- 90-132 sectors, 51 states using enhanced county business data and other private and public data. Identify interdependencies and possible interactions. Leads to goal of common operating picture	Greg Pompelli (ERS) pompelli@ers.usda.gov
		GIS platform for production, trade, processing, and assembly. Provide scope and context for events. Leads to goal of common	

Themes	Agency	Project	Point of Contact
		operating picture	
		Decision support epidemiology- economic modeling project- compares mitigation strategies and estimate economic effects and down stream effects for disease event. Leads to goal of common operating picture	
	DOI	Vulnerability of embankment dams to explosive attack: research being conducted with USACE and Sandia; Research includes physical scale modeling and computer modeling; research includes damage mitigation	Dave Achterberg (USBR)
		Vulnerability of concrete dams and operating features (spilling gates) to underwater attack by explosion: research conducted by Reclamation and Naval Surface Warfare Center; research includes scale modeling and computer simulation; research includes detection and damage mitigation	

Goals	Agency	Project	Point of Contact
1.6 Response, Recovery, and Reconstitution	DHS	United incident command and decision support innovative architectures	Peter Miller (S&T)
	DoD	Response and recovery technology for dams and locks	Will McMahon (USACE)
	EPA	Alternate supplies and decon work related to CB&R; Buildings and water systems	Alan Hais
	NSF	Infrastructure and Information Systems Program: advanced information systems and technologies to sustain physical infrastructure, hazard preparedness and response, and societal and economic impacts	Dennis Wenger
		Cyber Trust basic research- Internet response to worm/ virus attacks, system recovery and reconstitution	Carl Landwehr
	NIST	Evaluation and deployment guidelines of self healing Microwave relay networks for sensing, monitoring networks	Kate Remley (303) 497-3652
		Biological Mitigation Technologies: radiation treatment of mail, packages, etc.	Lisa Karam (301) 975-5561
		Standards and Performance metrics for US&R robots	Elena Messina Elena.messina@nist.gov

		Pipeline Safety: Measurements and standards for pipeline materials to access the extent of damage of an attack, either intentional or unintentional	Carol Handwerker (301) 975- 6158
		Advanced Fire Service Technologies: Information rich decision making; personnel protective gear; technologies (IR, imagers, locators); and, virtual firefighters training	William Grosshandler (301) 975-2310
		Simulation- based training for emergency responders	Al Wavering
	USDA	National Animal Health Laboratory Network: Response to outbreaks (surge capacity)	Bill Wagner (CSREES) wwagner@csrees.usda.gov and Larry Granger (APHIS) larry.m.granger@aphis.usda.gov
		Plant and animal genetics/ germ-plasm repository	Peter Brentting / Joe Spence
		Animal I.D.: ID of animals is critical in tracing animal movements during outbreaks	Valerie Ragan (APHIS) Valerie.ragan@aphis.usda.gov
		Survivability of threat agents in food matrices	Lynda Kelley (706) 546-3314
	Unknown	Emergency Responder training facility; and, self-diagnosing airplanes (i.e., MANPADS attack) autonomous recovery using advanced risk modeling, simulation, analysis	Unknown

Goals	**Agency**	**Project**	**Point of Contact**
1.7 New and Emerging Threats and Vulnerabilities	NASA	Risk based assessment of the aviation system (planes, airports, and systems)	Frank Jones (LANL) (757) 864-5271 and Mike Sorokach (757) 864-7143
		EME: Need to focus and create interagency working group	Terri Goodwin (650) 604-1700
	NSF	Network for Earthquake Engineering Simulation (NEES) seismic design, mitigation, and retrofit	Joy Pauschke
	DHS	Studies in emerging threats being preformed by HIS: GPS	John Cummings (S&T)

		vulnerabilities; HPM; and EMP	
		How to add subject matter to intel gathering?	Mike Lombard Mike.lombard@dhs.gov
	CIA	Threats based on access to technologists (scientists and engineers) such as identified by Marc Sageman in his book on Terrorist Networks	Fred Ambrose (703) 874-1003
	NIST	Microwave, non-wave, THz materials characterization including explosives, biologics, spectroscopy	Dennis Friday (303) 497- 3131

Themes	Agency	Project	Point of Contact
1.8 Advanced Infrastructure Architecture and Systems Design	DOT	Android model for cyber security- resilience/ self healing	Deborah Hermann (FAA)
		Inter-modal aspects of transportation security	Dr. Lewis Clopton & Dawn Tucker (FTA)
		Bridge specific blast loading program	Sheila Duwadi (FHWA)
		Standardized blast response curves for bridges	
		Blast testing of full-scale, pre-cast, pre-stressed concrete girder bridges	
		Development of anti-ram safety barriers	Michael Trentacoste (FHWA)
	NSF	Tera Grid as an advanced shared computing resource that is difficult to make secure	Guy Almes
		NEES	Joy Pauschke
		Future internet architecture	Guru Parulkar
		Secure wireless networking	Joe Evans
		Industry/ University Cooperative Research Centers: topics funded include cyber-protection, identification technology, and experimental computer systems	Alex Schwarzkopf
		Control systems, SCADA, sensor nets: System architectures, basic research in supervisory and multi-modal control, and software enabled control	Helen Gill
		Distributed real-time embedded systems research	
		Cyber Trust funds projects in more predictable, more accountable	

		and less vulnerable to attack; develop and train workforce, the public educated on ethical use	
		In collaboration with other agencies- future secure real-time operating systems architecture and middleware	Helen Gill, Carl Landwher, Brett Fleisch
	FAA	Free Flight Program has implications for security of National Airspace System	Did not provide
	NIST	Industrial control system security standards and test methods (including SCADA, electric power, etc)	Al Wavering wavering@nist.gov
		High Performance Advanced Materials: high performance structural materials; and, pseudo elastic materials	Carol Handwerker Carol.handwerker@nist.gov
	DOE	High temperature superconducting high voltage transformer	Phil Overholt (OETP)
	DoD	Homeland Defense Mission Assurance Portal	John P. Keenan (DPO-MA) Dahlgren
	NASA	Langley and Ames have an aviation safety and security program (focus on general aviation?)	Did not provide

Themes	Agency	Project	Point of Contact
1.9 Human and Social Issues	OSTP	Note: The NSTC Social, Behavioral, and Economic Sciences (SBE) Committee has a crosscut of all SBE programs and funding	Susan Brandon
	EPA	Communication strategies for drinking water and waste water utilities	Curt Baranowski
		Communication strategies for local governments for water and related "events"	
	DOI/USBR	Development of risk assessment modeling for diverse assets	Dave Achterberg
		Research on economic disaster modeling to determine direct and indirect economic cost and impacts of dam failures	
		Note: Research and development by Sandia National Lab	
	NSF	Human and social dynamics (HSD)- Agents of change, large scale transformations; dynamics of human behavior; decision making and risk	Rachel Hollander
		Cyber Trust- Privacy and technology; economics and technology	Carl Landwher/ Maria Zemankova

	NASA ARC	Human interface with technology	Terri Goodwin (650) 604-1700
	NIST	Economic consequence analysis- develop models and tools for life cycle cost analysis for Homeland Security technologies & mitigation practices; economic incentives; multi-hazard	Robert Chapman

Themes	Agency	Project	Point of Contact
1.10 Other	NIST	Metrology-(measurement techniques, calibrations, standard reference data) related to a broad range of CIP themes- i.e. measurement tracalibility	Dennis Friday
		Fire as a threat to physical infrastructure is not adequately addressed: wild land/ urban interface fires; terrorist/ arson fires; fire and chemicals; fire and blast. There is no place in DHS where basic research into fire and fire mitigation strategies are researched (as opposed to focused portfolios in chem., bio, and rad/nuc.	William Grosshandler (301) 975-2310
	DHS	Internet protocol priority service	Bill Ryan (NCS)
		Back-up dial tone analysis/ contingency communications	
		Internet disruption analysis	
		Cyber Security Portfolio: Cyber security testbed program; cyber security data sets program	Simon Szykman
	NASA	EME threats and countermeasures	Terri Goodwin/ Dr. John Beggs (757) 864-1829
	CIA DDS&T-ITIC	Basic/ applied S&T R&D addressing intel support needs for critical infrastructure, such as genomic research; sensors; etc	John Phillips (703) 874-0814
	FDA	Dose Response: Determine oral infectious dose of specific threat agents in food.	Dave Acheson
	DOS	International support for cooperative programs regarding S&T for Homeland Security and counter- terrorism	Dr. Stan Riveles (202) 647-6121

C-2 Strategic Goals

Goals	Agency	Project	Point of Contact
2.1 A national common operating picture for critical infrastructures	DOI – Bureau of Reclamation	• Vulnerability of concrete dams and operating features (spillway gates) to underwater or waterside explosive attacks. • Research being conducted by Reclamation and Naval Surface Weapons Center(s). • Research includes scale modeling and computer simulation. • Research includes defector and damage mitigation.	Dave Achterberg. Security, Safety and Law Enforcement
		• Vulnerability of embankment dams to explosive attack. • Research being conducted with Army Corp of Engineers and Sandia National Labs. • Research includes scale physical modeling and computer simulation. • Research includes damage mitigation.	
		• Development of risk assessment modeling for diverse assets. • Research and development by Sandia National Labs. • Research on economic disaster modeling to determine direct and indirect economic costs and impacts of dam failures.	
	NIST	Advanced Fire Service Technologies • Information-rich decision making • Personnel protective gear • Technologies (IR imagers, locators…) • Simulations and firefighter training	William Grosshandler (301) 975-2310
		• Sensor performance evaluator standards	
		Radiological/Nuclear • Protocols, testing/evaluations, interoperability standards, calibrations, SRMs (standards), NL leadership	Lisa Karam (301) 975-5561

Goals	Agency	Project	Point of Contact
		High Energy-Active Integration • Performance and safety standards, technology validation	
		Sensor network and standards (interoperability)	Al Wavering wavering@nist.gov
		Modeling and simulation, interoperability/integration, standards	
		Simulation-based training for emergency response	
	U.S. Army Corps of Engineers	Dams and navigation systems	Will McMahon
	DHS	BTS-Net	Jeanne.Lin@dhs.gov
		Unified Incident command and decision support innovative architectures	Peter Miller DHS S&T Program Manager
	USDA	Infrastructure: Agriculture diagnostic; lab networks and land grant university systems; standard ops	Kitty Cardwell, Bill Wagner, CSRees
	NRC	Vulnerability/risk analysis methods for complex scenarios (e.g. multiple assaults)	Mark Cunningham
	Dept of State	International support for cooperative programs re: S&T for Homeland security	Dr. Stan Riveles Rivelessa@state.gov 202-647-6121
	NASA	NASA developing COP for National Air Space	Terri Goodwin 650-604-1700
	FEMA	Risk Assessment Modeling Tools: HAZMAS-HM Software Tool (existing) • A loss estimation tool for natural hazards (EQ, Flood, Hurricane) with applicability to man-made hazards through existing interface capabilities and by linking to other tools through a GIS platform. (Large IT investment over 10 years)	Unknown

Goals	Agency	Project	Point of Contact
2.2 An inherently secure next-generation internet architecture	NSF	Tera Grid as an advanced cyber-infrastructure facility in need of the "secure next generation internet architecture".	Guy Almes
		NSF Middleware Initiative: (a growing set of middleware, much of it contributing to effective, scalable identify/authentication/authorization issues)	
		DDOS prevention architecture.	Carl Landwehr, Joe Evans Cyber Trust
	NIST	Standards and protocols for biometrics	Marty Herman Marty.herman@nist.gov
		Cyber security assurance for the private sector: R&D, standards, education	Paul Domich, Ed Roback
2.3 Resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems	NIST	Standards and protocols for biometrics	Marty Herman Marty.herman@nist.gov
		RFID chips – Passports and other applications. Security issues (security chip/devices – to prevent alteration)	Carol Handwerker (301) 975-6158
		Soft body armor standards: • Performance of vest materials • Performance of fragile bullets	
		High performance advanced materials: • Pseudo elastic materials • High performance structural materials	
		Advanced materials characterization methods for energy absorbing self healing materials: • NIST Center for Neutron Research • NIST Combustibles Methods Center • Mechanical prep under extreme conditions	
		Standards and performance metrics for US&R robots	Elena Messina Elena.messina@nist.gov
		Bioagent mitigation technologies: radiation treatment of mail, packages, etc…	Lisa Karam (301) 975-5561
		Safety of threatened buildings: • Increased structural integrity	William Grosshandler (301) 975-2310

Goals	Agency	Project	Point of Contact
		• High performance steel and fire resistance materials • Improving emergency Egress/access • Developing building equipment standards and guidelines	
		Industrial Control System Security Standards and Test Methods	Al Wavering wavering@nist.gov
	NSF	Future secure supervisory control/SCADA	Helen Gill
		Center for Internet Epidemiology. Center for security through interaction modeling Resilient/self-healing in cyber infrastructure system(s)	Carl Landwehr, Joe Evans Cyber Trust
	NASA	Cyber: NASA developing cyber security applications and methods to harden aviation networks and systems.	Terri Goodwin (650)604-1700
	DHS	Fast simulation and modeling of the electric distribution grid for detection and prevention of cascading failures	Peter Miller DHS S&T Program Manager
	NRC	Evaluation of impacts on concrete/steel structures (impacts involving explosives, vehicles, etc.)	Mark Cunningham NRC
	FEMA	Risk Management Series: FEMA Guidance Publications: • Ongoing program to develop guidance for design professionals and decision makers using state-of-the-art physical security knowledge/technology (in coordination with numerous government agencies and private sector groups. (Developed with modest budgets).	Unknown

APPENDIX D—PARTICIPANT LIST

Last Name	First Name	Agency	Title	Phone	E-mail
Arocho	Julio	Army Corps of Engineers	Assistant Director, Directorate of R&D	(202) 761-1849	Julio.E.Arocho@usace.army.mil
Ambrose	Fred	Central Intelligence Agency (CIA)			fredaz@ucia.gov
Landwehr	Carl	Computer and Information Science and Engineering (CISE), National Science Foundation	Program Director, Cyber Trust	703-292-8950	clandweh@nsf.gov
Roach	Lewis	Defense Threat Reduction Agency (DTRA)	Senior Advisor	703-325-7425	lewis.roach@dtra.mil
Robinson	Glenn	Defense Threat Reduction Agency (DTRA)		703-325-1078	glenn.robinson@dtra.mil
Santiago	Perfecto	Department of Agriculture (USDA), FSIS	Deputy Assistant Administrator	202-205-0452	perfecto.santiago@fsis.usda.gov
Shanahan	Mike	Department of Defense (DOD)/DPO-MA		540-653-7866	Michael.t.shanahan@navy.mil
Kenchington	Henry	Department of Energy (DOE)	Program Manager	202-586-1878	Henry.Kenchington@hq.doe.gov
Miller	John	Department of Energy (DOE)	Program Manager/SC	301-903-5866	John.Miller@science.doe.gov
Overholt	Philip	Department of Energy (DOE)			Philip.Overholt@hq.doe.gov
Soboroff	Mike	Department of Energy (DOE), Office of Energy Assurance	Infrastructure Analyst	202-586-4936	Mike.Soboroff@hq.doe.gov
Warwick	Marion	Department of Homeland Security		703-883-6658	mharring@mitre.org
Bradley	Mark	Department of Homeland			mark.bradley@dhs.gov

		Security (DHS)			
Fravel	Jeanne	Department of Homeland Security (DHS)			Jeanne.Fravel@dhs.gov
Hoyt	John	Department of Homeland Security (DHS)			john.hoyt@dhs.gov
Hynes	Mary Ellen	Department of Homeland Security (DHS)		202- 254-5807	MaryEllen.Hynes@dhs.gov
Lantzer	Paula	Department of Homeland Security (DHS)			paula.lantzer@dhs.gov
Lombard	Mike	Department of Homeland Security (DHS)	Director, CIP (Cyber) NCSD	703-235-5039	mike.lombard@dhs.gov
Long	Randy	Department of Homeland Security (DHS)			randy.long@dhs.gov
Szykman	Simon	Department of Homeland Security (DHS)			Simon.Szykman@dhs.gov
Wolff	Evan	Department of Homeland Security (DHS)			Evan.Wolff@dhs.gov
Brown	Dale	Department of Homeland Security (DHS), ICD	Sector Coordinator - Public Health	202-282-9545	dale.brown1@dhs.gov
Sauer	Robert	Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection		202-282-8764	robert.sauer@dhs.gov
Fleisher	Howard	Department of Homeland Security (DHS), Transportation Security Administration (TSA)		609-813-2751	howard.fleisher@dhs.gov
Brenner	Paul	Department of Homeland Security (DHS), IAIP	Contractor		pbrenner@icfconsulting.com
Vitko	John	Department of Homeland Security (DHS), Biological Countermeasures			john.vitko@dhs.gov

		Portfolio Manager			
Laatsch	Ed	Department of Homeland Security (DHS), FEMA	Chief, MES Section/Mitigation	202-646-3885	ed.laatsch@dhs.gov
Miller	Peter	Department of Homeland Security (DHS), HSARPA	Program Manager/CIP	202-254-6144	Peter.Miller@dhs.gov
Kennett	Milagros	Department of Homeland Security (DHS), Mitigation Division, EP&R, FEMA			Milagros.Kennett@dhs.gov
Hinkle	Chad	Department of Homeland Security (DHS), National Cyber Security Division	Strategic Initiatives	703-235-5175	Chad.Hinkle@dhs.gov
Waters	Laurie	Department of Homeland Security (DHS), Rad/Nuke Countermeasures Deputy Director		202-254-5732	Laurie.Waters@dhs.gov
Cummings	John	Department of Homeland Security (DHS), S&T	Director, CIP Portfolio	202-254-5805	john.cummings@dhs.gov
Buddemeier	Brooke	Department of Homeland Security(DHS), Emergency Preparedness & Response Portfolio Representative			brooke.buddemeier@dhs.gov
Ryan	Bill	Department of Homeland Security (DHS), National Communications System (NCS)	Engineer	703-607-6127	ryanw@ncs.gov

Gauthier	Paul	Department of Justice (DOJ)		202-616-9142	paul.e.gauthier@usdoj.gov
Riveles	Stan	Department of State Office of the S&T Adviser to the Secretary	Senior Counselor	202-647-6121	RivelesSA@state.gov
Achterberg	Dave	Department of the Interior (DOI), Bureau of Reclamation	Assistant Director , Security, Safety & Law Enforcement	303-445-2766	dachterberg@do.usbr.gov
Fowler	Dan	Department of the Interior (DOI), Office of Law Enforcement and Security, Security Division	Special Agent Office Law Enforcement & security Security Division	202-208-5108	Daniel_Fowler@ios.doi.gov
Devine	Jim	Department of the Interior (DOI), U.S. Geological Survey, Office of the Director			jdevine@usgs.gov
Pereti	Brian	Department of the Treasury			brian.peretti@do.treas.gov
Harrell	Jim	Department of Transportation (DOT), Office of the Chief Information Officer			Jim.Harrell@ost.dot.gov
Harnett	Kevin	Department of Transportation (DOT)	Cyber Security Program Manager	617-699-7086	harnett@volpe.dot.gov
Tucker	Dawn	Department of Transportation (DOT)		202-366-6532	Dawn.Tucker@ost.dot.gov
Marchessault	Tom	Department of Transportation (DOT), Research and Special Programs Administration	Associate Administrator for Innovation, Research, & Education	202-366-6373	Thomas.Marchessault@RSPA.dot.gov
Duwadi	Sheila	Department of Transportation (DOT), Federal Highway	Team Leader, Bridge Safety, Reliability & Security		Sheila.Duwadi@fhwa.dot.gov

		Administration			
Gerner	John	Department of Transportation (DOT), Federal Highway Administration			John.Gerner@fhwa.dot.gov
Allgeier	Steve	Environmental Protection Agency (EPA)			allgeier.steve@epamail.epa.gov
Hais	Alan	Environmental Protection Agency (EPA)	HQ Water Security Research Coordinator	202-564-9827	Hais.Alan@epamail.epa.gov
Herrmann	Jon	Environmental Protection Agency (EPA)	Director, Water Infrastructure Protection Division	513-569-7839	Herrmann.Jonathan@epamail.epa.gov
Oppelt	Tim	Environmental Protection Agency (EPA)	Director, National Homeland Security Research Center	513-569-7904	Oppelt.tim@epa.gov
Silverstein	Irwin	Environmental Protection Agency (EPA)	Environmental Engineer		Silverstein.Irwin@epamail.epa.gov
Wheeler	James	Environmental Protection Agency (EPA)	Environmental Engineer	202-564-6662	Wheeler.James@epamail.epa.gov
Baranowski	Curt	Environmental Protection Agency (EPA)		202-564-0636	Baranowski.Curt@epa.gov
Clark	Steve	Environmental Protection Agency (EPA)			Clark.Stephen@epa.gov
Jutro	Peter	Environmental Protection Agency (EPA)			Jutro.Peter@epamail.epa.gov
Herrmann	Deborah	Federal Aviation Administration (FAA)	Technical Advisor for Information Security		Debra.Herrmann@faa.gov
Greenberg	Bob	G&H International			rgreenberg@ghinternational.com
L'Heureux	Jamie	G&H International			jlheureux@ghinternational.com
Stoecker	Lindsay	G&H International		202-955-9503	lstoecker@ghinternational.com

Harrington	Michael	Health & Human Services (HHS)			
Lavin	Roberta	Health & Human Services (HHS), Office of Public Health Emergency Preparedness	Captain, HSPHA	202-205-4782	Roberta.Lavin@hhs.gov
Healey	Jason	Homeland Security Council			jhealey@who.eop.gov
Castagna	Michael	National Aeronautics & Space Administration (NASA)	IT Security Officer		michael.j.castagna@nasa.gov
Goodwin	Terri	National Aeronautics & Space Administration (NASA)		650-604-1700	teresa.m.goodwin@nasa.gov
Martin	Frank	National Aeronautics & Space Administration (NASA)	Chief Information Assurance Officer	202-358-0062	Frank.Martin-1@nasa.gov
Friday	Dennis	National Institute of Science & Technology (NIST), Electromagnetics Division 818	Division Chief		friday@boulder.nist.gov
Handwerker	Carol	National Institute of Science & Technology (NIST), Chief, Metallurgy Division	Chief, Metallurgy Division	301-975-6158	carol.handwerker@nist.gov
Remley	Kate	National Institute of Science & Technology (NIST), Electromagnetics Division 818	Division Technical Liaison	303-497-3652	remley@boulder.nist.gov
Cavanaugh	Richard	National Institute of Standards and Technology (NIST)	Chief, Surface & Microanalysis, Science Division	301-975-2368	richard.cavanagh@nist.gov

Domich	Paul	National Institute of Standards and Technology (NIST)	Associate Director, Building and Fire Research Laboratory	301-975-5624	domich@nist.gov
Gayle	Frank	National Institute of Standards and Technology (NIST)	Materials Science & Engineering Laboratory	301-975-6161	frank.gayle@nist.gov
Grosshandler	William	National Institute of Standards and Technology (NIST)	Division Chief	301-975-2310	wgrosshgandler@nist.gov
Karam	Lisa	National Institute of Standards and Technology (NIST)	Acting Division Chief Ionizing Radiation Division	301-975-5561	lisa.karam@nist.gov
Wavering	Al	National Institute of Standards and Technology (NIST)	Chief, Intelligent Systems Division	301-975-3461	albert.wavering@nist.gov
Almes	Guy	National Science Foundation (NSF)	Program Director for Terra Grid	703-292-7898	galmes@nsf.gov
Buckius	Richard	National Science Foundation (NSF)	Division Director, Chemical &Transportation	703-292-8370	rbuckius@nsf.gov
Cherniavsky	John	National Science Foundation (NSF)			jcherniavs@nsf.gov
Clegg	Andrew	National Science Foundation (NSF)	Program Director	703-292-4892	aclegg@nsf.gov
Deshmukh	Abhijit	National Science Foundation (NSF)	Program Director	703-292-7061	adeshmukh@nsf.gov
Figueroa	Juan	National Science Foundation (NSF)	Program Manager	703-292-7054	jfiguero@nsf.gov
Fragaszy	Richard	National Science Foundation (NSF)	Program Manager	703-292-7011	rfragasz@nsf.gov
Gill	Helen	National Science Foundation (NSF)			hgill@nsf.gov
Jameson	Leland	National Science	Program Officer	202-292-4883	ljameson@nsf.gov

		Foundation (NSF)			
Janini	George	National Science Foundation (NSF)	Program Director	703-292-4972	gjanini@nsf.gov
Lempert	Rick	National Science Foundation (NSF)			rlempert@nsf.gov
McCabe	Steve	National Science Foundation (NSF)			smccabe@nsf.gov
Nelson	Priscilla	National Science Foundation (NSF)			pnelson@nsf.gov
Pauschke	Joy	National Science Foundation (NSF)	Program Director	703-292-7024	jpauschk@nsf.gov
Ferris	John	Occupational Safety and Health Administration (OSHA), Office of the Assistant Secretary	Special Assistant for Emergency Preparedness & Response	202-693-1973	Ferris.John@dol.gov
Abrahms	Andy	Office of Management & Budget (OMB)			andrew_abrahms@omb.eop.gov
Holm	Jim	Office of Management & Budget (OMB)			james_holm@omb.eop.gov
Hunn	Eric	Office of Management & Budget (OMB)	Homeland Security Branch	202-355-3494	Eric_Hunn@omb.eop.gov
Wachter	Ralph	Office of Naval Research		703-696-4304	wachter@onr.navy.mil
Hays	Sharon	Office of Science and Technology Policy (OSTP)			Sharon_L._Hays@ostp.eop.gov
Romine	Charles	Office of Science and Technology Policy (OSTP)		NSTC Agency Representative	cromine@ostp.eop.gov
Voeller	John	Office of Science and Technology Policy (OSTP)		816-853-7839	voellerjg@bvsg.com
Whitney	Gene	Office of Science and Technology Policy (OSTP), National Science and			gwhitney@ostp.eop.gov

		Technology Council			
Bradshaw	Steve	Office of Secretary of Defense (OSD)	MILCON Chief, AT & FP Chief	703-697-8050	Steve.Bradshaw@osd.mil
Wilson	Richard	Office of the Deputy Under Secretary of Defense		703-588-7417	Richard.Wilson@osd.mil
Black	Steve	Office of the Vice President	Special Advisor	202-456-6486	sblack@ovp.eop.gov
Thomas	Stephen	Secretary of the Air Force (SAF)/AQRT			stephen.thomas@pentagon.af.mil
Penderson	Perry	Technical Support Working Group (TSWG)			pedersonp@TSWG.GOV
Agan	Sarah	Touchstone Consulting	Principal Consultant	202-449-7247	sarah.agan@touchstone.com
Dye	Cindy	Touchstone Consulting	Director, Public Safety	202-338-2525	cindy.dye@touchstone.com
Elder	Erin	Touchstone Consulting	Consultant	202-449-7216	erin.elder@touchstone.com
Espinosa	Julisa	Touchstone Consulting	Consultant	202-449-7218	espinosa.julisa@touchstone.com
McGoff	Chris	Touchstone Consulting	Chief Executive Officer	202-338-2525	chris.mcgoff@touchstone.com
Prater	Ron	Touchstone Consulting	Director, Public Safety	202-339-0288	ron.prater@touchstone.com
Mosher	Reed	US Army Corps of Engineers	Technical Director	601-639-3956	reed.l.mosher@erdc.usace.army.mil
Garris	Glen	US Department of Agriculture (USDA), APHIS		301-734-5875	glen.i.garris@usda.gov
Spencer	Denise	US Department of Agriculture (USDA), APHIS			denise.l.spencer@aphis.usda.gov
Spence	Joe	US Department of Agriculture (USDA), ARS			joseph.spence@nps.ars.usda.gov

Cardwell	Kitty	US Department of Agriculture (USDA), CSREES	National Program Leader Plant Pathology	202-401-1790	kcardwell@csrees.usda.gov
Wagner	Bill	US Department of Agriculture (USDA), CSREES		440-812-6416	wwagner@csrees.usda.gov
Pompelli	Greg	US Department of Agriculture (USDA), Economic Research Service	Project Leader/Economist	202-694-5353	pompelli@ers.usda.gov
Kelley	Lynda	US Department of Agriculture (USDA), FSIS			lynda.kelley@fsis.usda.gov
Maczka	Carole	US Department of Agriculture (USDA), FSIS			Carol.Maczka@fsis.usda.gov
Lay	William	US Department of Commerce	Director, IT Security, Infrastructure & Technology	202-482-4708	WLay@doc.gov
Acheson	David	US Food & Drug Administration (FDA)	Director, Food Safety Security	301-436-1910	david.acheson@fda.gov
Stambaugh	Margaret	US Nuclear Regulatory Commission (NRC)			mxs8@nrc.gov
Thomas	Eric	US Nuclear Regulatory Commission (NRC)	Emergency Response Coordinator	301-415-6772	ext1@nrc.gov
McKirgan	John	US Nuclear Regulatory Commission (NRC), Division of Nuclear Security			jbm4@nrc.gov
Orders	William	US Nuclear Regulatory Commission (NRC), Division of Nuclear Security			wxo@nrc.gov

Cheok	Michael	US Nuclear Regulatory Commission (NRC), Incident Response Directorate, Office of Nuclear Security and Incident Response	Deputy Director		mcc2@nrc.gov
Cunningham	Mark	US Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research, Division of Risk Analysis & Applications	Deputy Director Division of Rick & Analysis	301-415-5790	mac3@nrc.gov