2008–2009 NSTAC Reports

"NSTAC: Enhancing National Security and Emergency Preparedness through Communications"

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

2008–2009 NSTAC Reports

June 2009

Table of Contents

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

2008 Research and Development Exchange Workshop Proceedings

Evolving National Security and Emergency Preparedness Communications in a Global Environment

September 25-26, 2008
Motorola Innovation Center, Schaumburg, Illinois

Memorandum for the Industry Executive Subcommittee

Subject: 2008 Research and Development Exchange Workshop Proceedings

On September 25-26, 2008, the Industry Executive Subcommittee's (IES) Research and Development Task Force (RDTF), of the President's National Security Telecommunications Advisory Committee (NSTAC), held the eighth Research and Development Exchange (RDX) Workshop, at the Motorola Innovation Center in Schaumburg, Illinois. The purpose of the event was to:

1. Stimulate and facilitate discussion between participants from industry, Government, academia and the public safety sector on the national security and emergency preparedness impact of the evolving communications environment;

2. Explore and discuss important research and development (R&D) efforts in the area of communications that could alter the industry and the role it plays in various critical infrastructure activities;

3. Provide input to the U.S. Office of Science and Technology Policy (OSTP), the U.S. Department of Homeland Security (DHS), and the U.S. Department of Defense (DOD) to help inform their research agenda development processes and budgetary decisions;

4. Identify and characterize barriers and challenges to exploiting evolving communications to address national security and emergency preparedness (NS/EP) concerns; and

5. Develop new and innovative approaches for Government and industry to deal with current and future communications technology policy matters.

Participants engaged in discussion and debate not only during breakout and plenary sessions but also during their breaks and meals. All contributions were "not-for-attribution" unless specifically approved by the contributor. The participants collectively identified and characterized the following issues affecting the evolving communications landscape: (1) need for enhanced education, awareness, and training to reduce security risks and vulnerabilities; (2) need for economic justifications and incentives to drive R&D efforts in the business community; (3) need for survivable and resilient communications infrastructure during emergency situations; (4) challenges presented by expanded mobile architecture on access and trust; (5) need for evolving policy approaches to address the impacts of many new technologies; (6) need for increased investment in R&D infrastructure to drive R&D efforts; and (7) need for enhanced information sharing between industry, Government, and academia on impending threats and existing R&D efforts.

The insights, conclusions, and suggestions contained within these Proceedings result from the RDX Workshop and are solely attributable to the combined and unique contributions of RDX Workshop participants and invited speakers. The results indicate that the IES and the NSTAC should continue to work with DHS, DOD, OSTP, other NSTAC stakeholders, and international counterparts to explore key issues related to R&D of telecommunications and information systems that underpin key NS/EP functions.

The RDTF greatly appreciates the support of DHS and our breakout session facilitators. In particular, we would like to thank Ms. Susan Alexander, Chief Technology Officer, Information and Identity Assurance Office of the Assistant Secretary of Defense, Networks and Information Integration/DOD, Chief Information Officer; Mr. Gregory T. (Greg) Garcia, Assistant Secretary for Cyber Security and Communications, DHS; Dr. Chris Greer,

Director, National Coordination Office for Networking and Information Technology Research and Development; Mr. James Madon, Director and Deputy Manager, National Communications System, DHS; Dr. Douglas Maughan, Program Manager for Cyber Security R&D, Science and Technology Directorate, DHS; Dr. Veena Rawat, President of the Communications Research Centre Canada, Industry Canada; Ms. Leslie Ann Sibick, Chief, Research and Development Analysis/National Infrastructure Simulation and Analysis Center, Office of Infrastructure Protection, DHS; and Ambassador Richard Russell, Associate Director and Deputy Director for Technology, OSTP, Executive Office of the President, for their personal engagement in the event, which greatly contributed to its success. We would like to acknowledge the contributions of Mr. Greg Brown, President, Chief Executive Officer and NSTAC Principal, Motorola, Inc., and Mr. Gary Grube, Senior Fellow, Government and Public Safety, Motorola, Inc. We are also grateful to the staff for their outstanding work and attention to detail in making the event a success. Finally, we extend many thanks to the NSTAC member companies for their resources and support.

Respectfully,

Guy L. Copeland, CSC
Chair, Research and Development Task Force

Acknowledgements

The Research and Development Task Force (RDTF) of the President's National Security Telecommunications Advisory Committee would like to thank the representatives from industry, Government, and academia who participated in the eighth Research and Development Exchange (RDX) Workshop held at the Motorola Innovation Center on September 25-26, 2008, in Schaumburg, Illinois. The RDTF would especially like to acknowledge the important contributions of the Department of Defense (DOD), the Department of Homeland Security (DHS), Industry Canada, and the Office of the Manager, National Communications System for the planning and execution of the 2008 RDX Workshop.

A special thanks to the Workshop Moderators, Ambassador Richard Russell, Associate Director and Deputy Director for Technology, Office of Science and Technology Policy, Executive Office of the President; Ms. Susan Alexander, Chief Technology Officer, Information and Identity Assurance, Office of the Assistant Secretary of Defense, Networks and Information Integration/DOD, Chief Information Officer; Dr. Veena Rawat, President of the Communications Research Centre Canada, Industry Canada; and our invited speakers, Mr. Greg Brown, President and Chief Executive Officer, Motorola, Inc.; Mr. Gary Grube, Senior Fellow, Government and Public Safety, Motorola, Inc.; Mr. Gregory T. Garcia, Assistant Secretary for Cyber Security and Communications, DHS; Ms. Leslie Ann Sibick, Chief, Research and Development Analysis/National Infrastructure Simulation and Analysis Center, Office of Infrastructure Protection, DHS; Dr. Douglas Maughan, Program Manager for Cyber Security Research and Development, DHS Science and Technology Directorate; Dr. Chris Greer, Director, National Coordinating Office for Networking and Information Technology Research and Development; and Mr. James Madon, Director and Deputy Manager, National Communications System, DHS.

We would also like to extend our sincere appreciation to our breakout session co-facilitators, Ms. Peggy Matson, Motorola; Mr. Dan Phythyon, Office of Emergency Communications; Mr. Patrick Beggs, DHS; Mr. Jim Mathis, Motorola; Mr. Robert Dix, Juniper Networks; Mr. Robert Leafloor, Industry Canada; Mr. James Zok, CSC; Mr. Anthony Rutkowski, VeriSign; Mr. Siafa Sherman, Nortel Networks.

Table of Contents

Executive Summary

From September 25–26, 2008, the President's National Security Telecommunications Advisory Committee (NSTAC) conducted its eighth Research and Development Exchange (RDX) Workshop entitled, Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment. The purpose of the event was to stimulate an exchange of ideas among researchers, operational users, and executives from Government, industry, and academia focused on the full range of research and development (R&D) issues affecting NS/EP communications networks, advance the security of free nations, and enhance preparedness and response activities across sectors.

Dramatically changing business models of traditional telecommunications carriers, along with new technologies, are accelerating the advancement of global communications networks. The scale, scope, and character of the global next generation networks will revolutionize the planning, prioritization, and delivery of NS/EP communications. The 2008 RDX Workshop addressed a variety of high-level concerns that are affecting the communications and cyber environment and the way those concerns could alter NS/EP efforts.

The goal of the event was to gather valuable information from the assembled experts that the NSTAC's Research and Development Task Force (RDTF) could use to assist in developing proposed Presidential recommendations for the NSTAC. The R&D community's feedback will be helpful to the NSTAC and other key Government agencies in: (1) framing key policy issues surrounding R&D efforts relevant to NS/EP communications; (2) discussing how stakeholders can cooperate and coordinate efforts as communities of interest shift; (3) providing insights to the Office of Science and Technology Policy (OSTP), Department of Homeland Security, and Department of Defense (DOD) as they formulate research agendas and budget submissions; and (5) develop an agenda for action.

These Proceedings represent the discussions, ideas and final thoughts of the RDX Workshop attendees but the suggestions provided herein are not consensus and are not an official position of the NSTAC, the RDTF or its members. The document will be widely distributed and made available on the Office of the Manager, National Communications System website for reference and download by other NSTAC task forces and Government agencies.

Specifically, the event participants examined five focused areas:

- **Emergency Communications Response Networks:** Modernizing and updating emergency communications to meet interoperability, resiliency, and reliability requirements while recognizing the challenges presented by existing legacy systems, technological hurdles, limited funds, disparate standards, and a disparate stakeholder community.

- **Convergent Technologies:** Ensuring interoperability among new and legacy technologies, defining interoperability standards across networks, mitigating problems associated with network congestion, enabling network security, and ensuring network survivability for NS/EP communications in a converged environment.

- **Defending Cyberspace:** Promoting the need for research to understand the increased vulnerabilities and threats to cyberspace and determining the most appropriate offensive and defensive technological and policy approaches to network security.

- **Identity Management:** Exploring R&D efforts that leverage existing identity management technologies and policies to ensure identification and authentication of network users and machines in an NS/EP event.

- **Emerging Technologies:** Examining emerging technologies to determine their potential impacts and identifying tools or policies to address the rising security issues presented by the evolving communications environment.

During the two-day event, participants engaged in a facilitated dialogue including both plenary and breakout sessions. From these sessions, seven overarching themes emerged:

- **Enhanced education, awareness, and training will reduce security risks and vulnerabilities.** Today's communications networks, information systems, and threat environment have evolved dramatically, resulting in the need for more robust education, awareness, and training programs to educate end-users and system developers alike on security risks and potential mitigation strategies. University programs need to enhance curriculum to teach aspiring developers secure coding and other security measures. Furthermore, service providers and manufacturers that provide equipment and services in support of NS/EP communications need to integrate security into systems development life cycles through training and education. R&D bodies, within industry, academia, and Government, need to work together to build increased awareness, coordination, and alignment of ongoing identity management (IdM) standards and R&D work. Finally, the user and standards bodies communities need to enhance outreach regarding security precautions to end-users because in today's converged technology environment many diverse devices are accessing the network and much of the responsibility for security and access control resides with the user.

- **Economic justifications and incentives need to drive R&D efforts in the business community.** The private sector often makes R&D decisions based on the perceived return on investment. Without a viable business case based on user requirements and market drivers, corporate entities are unlikely to pursue specific R&D investments. Any deferment of investment in technologies that may advance NS/EP communications by industry inhibits technological progress and in some cases exposes critical infrastructure and key resources to vulnerabilities. It is important for the Federal Government to provide incentives to industry to implement new technologies. An example discussed in the RDX Workshop was the need to identify business cases and models to support pervasive IdM use. Government efforts to encourage industry adoption of specific security methods should consider the business demands of private companies and ensure that there is a balance between profit expectations and expectations for technology investment.

- **The communications infrastructure must be survivable and resilient during emergency situations.** The collective desired characteristics of a sound emergency communications system are operability, interoperability, reliability, resiliency, redundancy, scalability, security, and efficiency. The development of network elements that require less power or use alternative power sources will increase the survivability and resiliency of networks during emergency situations. Currently, there is a need for new scalable and extendible architectures with better forensics that utilize distributed and portable energy technologies to support long-term NS/EP strategies and operations.

- **Expanded mobile architectures present challenges related to access and trust for NS/EP users.** An expanded mobile architecture where more intelligence and access points reside at the edge of the network is very prevalent in today's wireless infrastructure. Wireless technology companies have developed significant numbers of affordable mobile device that enable authentication and roaming across systems. These advancements inherently produce a more vulnerable system because of the widespread network accesses. Technologies for establishing interoperability and common credentials are critical. In the wireless network environment, there is a need for a trusted mobile computing platform to support NS/EP needs. In addition to this platform, a priority access framework for users and applications also needs to be developed.

- **Evolving policy approaches need to address the impacts of many new technologies on NS/EP communications.** Recent advancements in technology have brought about significant change; as a result, Government may need to update some

policies and regulations to keep pace with the evolving landscape. Some specific areas include the need for policy makers to determine the impacts of new technologies on privacy and the impact of privacy rules on NS/EP communications needs. Regulators need to explore setting baseline standards to enhance accountability in cyberspace and to address authority and jurisdiction as well as international acceptance of laws through federated entities and standards bodies. In addition, regulators need to make a paradigm shift in spectrum management and address the processes, regulations, and policies surrounding spectrum allocation and management.

- **Increased investment in R&D infrastructure needs to drive future R&D efforts.** To accomplish the strategies to support evolving NS/EP communications, key stakeholders much establish laboratories and pilot programs that drive new technologies for public safety. Beyond funding, there needs to be a coordinated effort across Government, industry, and academia to meet NS/EP communications challenges. Some examples for research and development projects that need additional funding are research into providing authentication at Layers 2 and 3 of the open system interconnection model, behavioral science models; and additional tools to identify the life cycle of malware systems.

- **Enhanced information sharing needs to occur between industry, Government, and academia on impending threats and existing R&D efforts.** Stakeholders need to have greater agreement and increased collaboration in order to meet the demands of the evolving NS/EP communications environment. The critical challenge is to engage industry, Government, and academia, as well as end-users in exchanging information about existing initiatives and challenges, thus facilitating the development of comprehensive solutions. Each party needs to share information regarding emerging technologies, interoperable and reciprocal trust mechanisms, vetting processes, audit regimes, and the real-time sharing of actionable threat information. This collaboration needs to take place locally, nationally, and internationally for emergency events.

During the plenary closing session, Dr. Veena Rawat, President of the Communications Research Centre Canada, Industry Canada; Ms. Susan Alexander, Chief Technology Officer, Information and Identity Assurance Office of the Assistant Secretary of Defense, Networks and Information Integration/DOD, Chief Information Officer; and Ambassador Richard Russell, Associate Director and Deputy Director for Technology, OSTP, Executive Office of the President commented on the results of the breakout sessions and challenged the RDX Workshop participants to focus on providing economic justification and metrics for proposed R&D investments.

1 Introduction

The Industry Executive Subcommittee's Research and Development Task Force (RDTF) is part of the National Security Telecommunications Advisory Committee (NSTAC), a Presidential advisory committee established in 1982 to provide the President with industry advice on national security and emergency preparedness telecommunications issues. From September 25–26, 2008, the RDTF held its eighth Research and Development Exchange (RDX) Workshop titled *Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment.*

1.1 Background

Dramatically changing business models of traditional telecommunications carriers, along with new technologies, are accelerating the advancement of global communications networks. The scale, scope, and character of the global next generation networks will revolutionize the planning, prioritization, and delivery of NS/EP communications. Given this evolving market and technology environment, the Workshop participants addressed the need for collaboration to preserve and enhance network security through targeted research and development (R&D) approaches. The two-day event featured keynote speakers and breakout sessions focused on the full range of R&D issues associated with ensuring NS/EP activities within the evolving communications and cyber landscape. Specifically, the participants explored five different issues concerning the communications infrastructure and its support of NS/EP activities:

- **Emergency Communications Response Networks:** Modernizing and updating emergency communications to meet interoperability, resiliency, and reliability requirements while recognizing the challenges presented by existing legacy systems, technological hurdles, limited funds, disparate standards, and disparate stakeholder communities.

- **Convergent Technologies:** Ensuring interoperability among new and legacy technologies, defining interoperability standards across networks, mitigating problems associated with network congestion, enabling network security, and ensuring network survivability for NS/EP communications in a converged environment.

- **Defending Cyberspace:** [1] Promoting the need for research to understand the increased vulnerabilities and threats to cyberspace and determining the most appropriate offensive and defensive technological and policy approaches to network security.

- **Identity Management:** Exploring R&D efforts that leverage existing identity management technologies and policies to ensure identification and authentication of network users and machines in an NS/EP event.

- **Emerging Technologies:** Examining emerging technologies to determine their potential impacts and identifying tools or policies to address the rising security issues presented by the evolving communications environment.

1.2 Purpose

The RDX Workshop facilitated an exchange of ideas among researchers and practitioners from academia, industry, and Governments on critical issues related to NS/EP communications. To stimulate robust discussion, facilitators and participants from the vendor, network provider, academic, and Government communities presented their viewpoints. The event gathered valuable information, observations, and conclusions from the assembled experts that could inform key Government stakeholders on these issue areas as they devise research agendas and budgetary decisions. Further, the NSTAC will use these Proceedings to inform its research agenda development and future work-plans. The Proceedings will be widely distributed and made available on the Office of the Manager, National Communications System (NCS) website for reference and download by other NSTAC task forces and Government agencies.

1.3 Proceedings Organization

This Proceedings document provides an overview of the 2008 RDX Workshop. Specifically, the five sections and associated appendices are:

- Section 1 presents background information on the 2008 RDX Workshop;
- Section 2 reviews the opening plenary session, including:
  - Welcoming remarks from Mr. Guy Copeland, CSC and RDTF Chair, and Mr. Greg Brown, President and Chief Executive Officer, Motorola;
  - Statements delivered by the co-moderators, Ambassador Richard Russell, Associate Director and Deputy Director for Technology, Office of Science and Technology Policy, Executive Office of the President; Ms. Susan Alexander, Chief Technology Officer, Information and Identity Assurance, Office of the Assistant Secretary of Defense, Networks and Information Integration/ Department of Defense, Chief Information Officer; Dr. Veena Rawat, President of the Communications Research Centre Canada, Industry Canada; and
  - Remarks and presentations from Mr. Gary Grube, Senior Fellow, Government and Public Safety, Motorola, Inc.; Mr. Gregory T. Garcia, Assistant Secretary for Cyber Security and Communications, Department of Homeland Security (DHS); Ms. Leslie Ann Sibick, Chief, Research and Development Analysis/National Infrastructure Simulation and Analysis Center, Office of Infrastructure Protection, DHS; Dr. Douglas Maughan, Program Manager for Cyber Security Research and Development, DHS Science and Technology Directorate; Dr. Chris Greer, Director, National Coordinating Office for Networking and Information Technology Research and Development; and Mr. James Madon, Director and Deputy Manager, NCS, DHS.
- Section 3 captures the observations and conclusions from the breakout session discussions;
- Section 4 highlights discussions from the closing plenary session;
- Section 5 presents the major conclusions from the 2008 RDX Workshop; and
- Appendices A–F includes the RDX Workshop agenda, speakers' presentations and biographies, and other materials.

2 Opening Plenary Session

The opening plenary session to the 2008 Research and Development Exchange (RDX) Workshop commenced with remarks from Mr. Guy Copland, CSC and Research and Development Task Force (RDTF) Chair. Mr. Copeland welcomed participants, specifically noting the importance of international participation with representatives from the United States and Canada. He emphasized the need to address international collaboration on the full range of national security and emergency preparedness (NS/EP) research and development (R&D) issues. Mr. Copeland noted that the current financial and political climate, as well as recent natural disasters, provides a timely and unique opportunity to identify and prioritize critical R&D requirements collaboratively. Mr. Copeland thanked participants for their attendance and encouraged them to focus discussions on providing actionable suggestions that key decision makers concerned with improving security, preparedness, and response efforts both within and across borders can implement.

2.1 Welcoming Remarks – Mr. Greg Brown

Mr. Copeland introduced Mr. Greg Brown, Chief Executive Officer, Motorola. Mr. Brown welcomed the participants to Motorola and expressed his appreciation to all involved with planning the RDX Workshop. He expressed that the scope and scale of global markets and networks drives the importance of addressing R&D collaboratively and across international boundaries. Mr. Brown expressed hope for a robust exchange of ideas among the participants during the RDX Workshop on a full range of issues affecting communications and enhancing NS/EP needs.

Mr. Brown noted the importance of innovation and research to enabling NS/EP communications and described people as the key to driving R&D progress. Mr. Brown concluded his thoughts by suggesting

potential discussions during the RDX Workshop could positively affect future R&D decisions related to communications.

2.2 Introductory Remarks – Mr. Gary Grube

Mr. Copeland introduced Mr. Gary Grube, Senior Fellow, Government and Public Safety, Motorola. Mr. Grube welcomed participants to the Workshop and to Motorola. He explained that his remarks would address issues and thoughts on the changing communications technology environment that would aid in fueling the breakout session discussions. He began his presentation by noting two statistics regarding the birth rate and mobile phones growth rate across the world to illustrate that the introduction and use of mobile communications devices are occurring at an extremely rapid pace.

Mr. Grube highlighted several technology shifts that are having a major impact on the field of communications and would be important to the breakout session discussions. He stated that the World Wide Web was the most important thing to happen to the field of communications. He explained that the Internet has allowed the shift from centralized communications to more usercentric activities that enable greater access to information. Internet business models based on peer-to-peer content sharing services are thriving. Next, he discussed the importance of the development of broadband or highspeed Internet capabilities. He stated that today's Internet provider services focus on providing access to high-speed, mobile fixed communications. He noted the importance of optical fiber networks to the future of mobile broadband communications because of its high bandwidth capabilities and low latency. He also raised the issue of spectrum allocation and the need for more available spectrum as well as technologies that improve efficiency of spectrum usage.

Mr. Grube identified cloud computing as a third technology shift that would alter communications. Cloud computing is the concept of using Web applications or software as a pay as you go service which also provide offline storage capabilities. He explained that cloud computing allows organizations to switch from their own hardware and software infrastructure to pay-per use models. He then discussed the way in which today's devices are incorporating more applications and modes within a single device. These devices improve efficiency and selfactualization for users while pushing the intelligence to the edge of the network and into the user's hand. He explained that these devices enable greater management of knowledge, which includes communication, search, data storage and recall, analysis, presentation, and decision-making capabilities. Finally, he noted that the Internet and faster connection speeds amplify the importance of digital content and social networking applications. With the new commercial communications world, content eclipses access as the driver of revenue.

Mr. Grube concluded his remarks by stating that the R&D community faces the challenge of increasing the value and utility of communications devices by increasing efficiency and usefulness while maintaining costs. He identified three approaches to leveraging new technologies: (1) create new assets; (2) extract continued value from current assets; and (3) enable improved process and policies.

2.3 Workshop Overview and Goals – Mr. Copeland

Mr. Copeland provided an overview of the President's National Security Telecommunications Advisory Committee (NSTAC) and its role in providing industry-based advice and expertise to the President related to NS/EP communications policy. Mr. Copeland noted that the goal of the RDX Workshop is to gather valuable information and constructive feedback that will inform the RDTF as it develops proposed Presidential recommendations for consideration by the NSTAC Principals. Next, he briefly described the history of the NSTAC's RDTF, indicating that the NSTAC has conducted several RDX Workshops with representatives from industry, Government, and academia since 1991 on a variety of important R&D topics related to NS/EP communications.

Mr. Copeland continued by describing the objectives for the 2008 RDX Workshop, commenting that the breakout session groups would: (1) explore and prioritize critical R&D requirements related to evolving NS/EP communications; (2) frame key policy issues surrounding R&D collaboration and make suggestions

on critical areas for further study by the NSTAC or international counterparts; (3) provide input to the Department of Defense (DOD), Department of Homeland Security (DHS), Office of Science and Technology Policy, and other key Government stakeholders as they prepare budget submissions and formulate research agendas; and (4) inform policymakers in their efforts to develop R&D priorities. Mr. Copeland concluded by reiterating the need for developing actionable suggestions for key stakeholders to carry forward.

2.4 Moderator's Address – Ms. Susan Alexander

Mr. Copeland introduced Ms. Susan Alexander, Chief Technology Officer (CTO), Information and Identity Assurance Office of the Assistant Secretary of Defense, Networks and Information Integration/DOD, Chief Information Officer. Ms. Alexander expressed her appreciation for the opportunity to serve as a moderator and set the context for the breakout session discussions. She briefly described her position as one that requires her to address a convergence of interests and noted that in addition to her role as CTO, she is actively involved in the Comprehensive National Cyber Security Initiative (CNCI). She noted that there are two initiatives under the CNCI, which single out R&D. Specifically, CNCI Initiative 4 addresses coordinating research across the Federal Government and Initiative 9 calls for the development of "leap-ahead" technology to mitigate the risks associated with the United States' strong reliance on cyber assets.

Ms. Alexander described the history of the DOD net-centric warfare program and explained how information can become a double-edged sword as adversaries attempt to exploit it for their own purposes. As DOD has acquired more experience with net-centricity, it has learned that it must consider carefully how it will protect and defend access to the information on which it is depending. She provided this story as real-life context for participants to consider when developing suggestions. Ms. Alexander asserted that playing defense is hard today and challenged the group to think in the following way: "if you are in a game you cannot win, then change the game." She offered, for example, that the best way to reduce risk is not always to remove vulnerabilities. That may be too hard. Risk can also be reduced by limiting the consequences of the attack or by eliminating the threat at its source. She provided a re-ordered approach to computer network defense: (1) keep the mission going; (2) determine how to respond and reconstitute quickly in case of an attack; and (3) identify the vulnerabilities and new protection strategies. She reinforced that in any risk-mitigation strategy ensuring the mission should be the prime responsibility.

Ms. Alexander went on to provide guidance on how participants should approach the breakout session discussions. She noted that many conference suggestions are not implemented because they do not provide actionable advice and conclusions. She encouraged the group to describe the specific goal of each suggestion and what it would look like if implemented, and to identify the steps that need to be taken to achieve successful implementation of the suggestion. She asked participants to put themselves in the place of the person receiving the suggestions and consider what information he or she would need to have in order to act. She highlighted the *Defending Cyberspace* breakout session and suggested participants in this session focus on defining the current state of affairs and identifying policy and technological approaches that would alter the current threat environment.

Ms. Alexander closed by discussing the upcoming National Cyber Leap Year initiative under the CNCI which is intended to identify the most promising game-changing ideas with the potential to reduce the Nation's vulnerabilities to cyber exploitations. She encouraged RDX Workshop attendees to respond to the request for input at www.nitrd.gov.

2.5 Address – Dr. Veena Rawat

Mr. Copeland introduced Dr. Veena Rawat, President of the Communications Research Centre Canada (CRC), Industry Canada. Dr. Rawat thanked the NSTAC for the opportunity to speak at her second RDX Workshop. She stated that CRC performs in Canada a combination of the activities carried out for the United States by the Federal Communications Commission (FCC), National Telecommunications and Information Administration labs and some of the

activities of Defense Advanced Research Projects Agency. CRC is responsible for conducting R&D on communications technologies and systems including wireless, broadcasting, and fiber. The agency provides technical support to the Canadian Government for the development of telecommunications standards and regulation and gives independent advice on science and technology policies. It also supports other Government agencies in their R&D efforts.

Dr. Rawat identified CRC's core competencies: wireless systems, communication networks, radio fundamentals, interactive multimedia (such as broadcasting technologies), and photonics. Work on the core competencies is organized into six major strategic priorities: (1) radio spectrum; (2) broadband; (3) applications; (4) defense communications; (5) network security and public safety; and (6) Internet/convergence policy. The Centre focuses on research, development, and promotion of all communications technologies.

Dr. Rawat described public safety and emergency preparedness communications as one of the key research areas for CRC. Currently, first responders use a variety of radio communications systems and dedicated and commercially provided systems, presenting interoperability challenges. CRC conducts research to address the interoperability requirements for emergency communications across responder groups and to examine the ability to transmit voice, video, or data across available bandwidth while maintaining reliability and security. She also discussed emerging trends within the communications field, including the need for ubiquitous wireless services anywhere, anytime. In addition, the convergence of cellular and fixed wireless access and location-awareness or global positioning system services is transforming communications because they enable users to customize the network to their needs. She noted that these communications trends have the potential to be useful and important in the area of public safety. Within the area of broadcasting, traditional platforms like over-the-air, cable, and satellite, are facing competition from emerging methods like mobile television, Internet television, and Internet protocol television. She suggested that broadcasting technologies have possibilities for emergency response in the area of emergency alerts over wireless. Additionally, she suggested that emergency managers could use satellite in search and rescue efforts and as a back-up communications system.

Dr. Rawat also addressed the growing demand for radio spectrum for mobile wireless access and multimedia services. Since radio spectrum is a limited resource, the only way to address the growing demand is through making more spectrum available or finding ways to use spectrum more efficiently. There is a need for R&D efforts on technologies that allow more intensive spectrum use, such as spectrum refarming, license exempt bands, spectrum sharing (which address the U.S. debate over white spaces), and dynamic spectrum access. She focused on software defined radio (SDR) and cognitive radio as two technology enablers that could significantly influence communications. Wireless sensor networks that include a network of distributed sensors to monitor physical and environmental conditions could have applications for security, monitoring, and detection activities. SDR, radio in which some physical layer functions are software defined, has the ability to support multiple spectrum protocols simultaneously thereby improving interoperability and reconfigurability. SDR would enable an organization to design its system in a way that is constantly changing to utilize available spectrum. Radio has evolved from a non-adaptive technology to "cognitive radio," which is a fully adapting, selfmanaging technology that is capable of sensing and using available channels. All of these technology enablers have possible benefits for the public safety community if they are properly explored.

Dr. Rawat concluded by encouraging the exploitation of commercial technologies for other purposes, particularly in the public safety arena. She reinforced the fact that spectrum is limited; therefore, as the demand continues to grow a plan must be developed to ensure availability and most efficient use of the resource. She stated that R&D activities should focus on enabling the public safety community and helping them meet their requirements.

2.6 Moderator's Address – Assistant Secretary Greg Garcia

Mr. Copeland introduced Mr. Gregory Garcia, Assistant Secretary for Cyber Security and Communications, DHS. Mr. Garcia expressed his appreciation for the opportunity to address the group and noted his participation in previous RDX Workshops. Mr. Garcia emphasized the continued example the NSTAC sets of a successful public-private partnership. He discussed the NSTAC's role in providing advice to the Federal Government on critical NS/EP communications matters.

Mr. Garcia discussed his background as a former staff member of the U.S. House of Representatives Committee on Science and Technology, which successfully shepherded passage of the *Cyber Security Research and Development Act*. The premise of the Act was for the Federal Government to help fund basic, long-term, high-risk research. Mr. Garcia stated that, because the private sector may not undertake similar R&D due to the high-risk nature of such research, Federal funding for cybersecurity R&D is important. He also emphasized that Federal funding would help create the next generation of scientists and technologists.

Mr. Garcia then posed the following question to participants for consideration: "Why does the convergence of information technology and communications matter and how does this affect R&D?" Mr. Garcia stated that the transformation of the network to allow convergent technologies provides more open access, and thus, exposes traffic to more threats. This, as well as other vulnerabilities, creates complex risk scenarios for NS/EP communications.

Mr. Garcia then emphasized how critical the ability to communicate is to incident response efforts. He mentioned the importance for the Government to examine potential impacts of packet-based services on the delivery of NS/EP communications. Mr. Garcia acknowledged the work of the NSTAC to determine if network degradation or disruption could affect NS/EP traffic. He highlighted the NSTAC's previous findings as well as its short-term and long-term recommendations to the President in this area.

Mr. Garcia challenged the RDX Workshop participants to answer the question: "How can Government more effectively work with the private sector to enhance the security of the nation's critical infrastructure and key resources (CI/KR) networks?" Specifically, he stated that DHS would like participants to address how to leverage this collaboration to reduce vulnerabilities and enhance defensive strategies in cybersecurity. Mr. Garcia then outlined the areas where DHS is taking an active role and providing the leadership and resources to enhance technology research. Mr. Garcia continued by summarizing CNCI Initiatives 4 and 12.

Mr. Garcia explained to participants that DHS would rely upon the Trusted Internet Connection Initiative, the Einstein Program, and the United States Computer Emergency Readiness Team Operations Center to reduce cyber risks across the Federal Government enterprise. The interaction between these three components is critical to the success of the CNCI. He noted specific areas where he foresaw needing additional funding including: data collection, data fusion, data analysis, data visualization, data sharing, supply chain risk management, and industrial control systems.

Finally, Mr. Garcia provided an outline of the Information Technology Sector Specific Plan's R&D priorities, which include cyber situational awareness and response, forensics, identity management (authentication), intrinsic infrastructure protocols security, modeling and testing, control systems security, scalable and secure systems, and trust and privacy.

2.7 Presentation – Ms. Leslie Ann Sibick

Mr. Copeland introduced Ms. Leslie Ann Sibick, Chief, Research and Development Analysis/National Infrastructure Simulation and Analysis Center, Office of Infrastructure Protection (OIP), DHS. Ms. Sibick presented a briefing on the Research and Development Analysis Branch's infrastructure protection R&D process and priorities. She said it was an honor to speak at the RDX Workshop and explained that in her role she reports directly to Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, DHS. She stated that her presentation would focus on providing an overview of the *National Infrastructure Protection Plan* (NIPP) R&D process.

Ms. Sibick began by providing an overview of OIP, which was established in 2007 to evaluate and reduce risk to CI/KRs. She noted that OIP serves as a primary point of contact and proponent for the eighteen CI/KRs regarding risk mitigation. OIP currently supports crosssector efforts particularly through the CI/KR R&D Working Group which is co-chaired by the DHS OIP Infrastructure and Analysis and Strategy Division and the DHS Science and Technology (S&T) Infrastructure and Geophysical Division. This group provides a forum for sectors to discuss common areas of concern, collaborate on cross-sector R&D projects, and develop sector R&D relationships. She also noted that DHS has an extensive, collaborative R&D program that helps to develop technology and tools to assist the CI/KR sectors. The S&T R&D process has funding available for those interested in pursuing grants for R&D initiatives. She identified the Kentucky Critical Infrastructure Protection and Southeast Regional Resiliency Initiative as examples of recent OIP R&D collaboration and coordination.

Ms. Sibick discussed the vision, goal, and phases of the NIPP R&D requirements process. She identified the vision as developing a repeatable, honest, and defendable requirements program that mitigates long-term national homeland security risks. She reinforced the need to show quantitatively the value of the requirements. The process assists NIPP stakeholders in identification and articulation of strategic R&D requirements and then facilitates coordination with S&T and others to address those capability gaps. Lastly, the goal of the requirements process is to align sector needs with expertise in academia, research and analysis centers, S&T Centers of Excellence, and research consortia, as well as OIP-directed programs such as the National Infrastructure Simulation and Analysis Center. She also discussed the R&D prioritization methodology being implemented to align CI/KR sector capability gaps and to incorporate priorities. She emphasized the importance of developing a quantifiable process given limited R&D funds and the numerous areas of possible R&D investment. The intent of the risk-informed R&D prioritization methodology is to compare all gaps against critical infrastructure protection R&D themes, strategic homeland infrastructure risk assessment, and other criteria. She stated that the process will address cross-sector/multi-sector issues and homeland security-relevant issues that transcend sectors. The intended outcome of the methodology is an organized, cross-referenced, and prioritized annual R&D requirements list.

Ms. Sibick closed her presentation emphasizing the fact that DHS has funding available for R&D projects that focus on identified priority gaps. OIP efforts continue to focus on ensuring proper integration of legacy projects and implementing a process that will ensure that high priority issues are identified and addressed.

2.8 Presentation – Dr. Douglas Maughan

Mr. Copeland introduced Dr. Douglas Maughan, Program Manager for Cyber Security R&D, S&T Directorate, DHS. Dr. Maughan began by describing the mission of the S&T Directorate "to conduct, stimulate, and enable research, development, testing, evaluation, and timely transition of capabilities which distinguishes it from other agencies." He explained that the S&T R&D execution model incorporates input from internal and external sources, such as Federal customers, critical infrastructure providers, and other sectors to prioritize requirements. He discussed key cybersecurity program areas, including information infrastructure security, cybersecurity research tools and techniques, and next generation technologies.

Dr. Maughan noted that the R&D portion of the *National Strategy to Secure Cyberspace,* identified border gateway protocol (BGP), domain name server, and Internet protocol version 6 as three areas that require additional security work. He explained that the security and continued functioning of the Internet will be influenced in part by the success or failure of implementing more secure and more robust BGP and domain name system (DNS). He stated that there are development activities underway to address DNS, including a revised roadmap for deployment of the Domain Name System Security (DNSSEC) protocol that was published in March 2007 and development of a testbed by the National Institute of Standards and Technology. He referenced a memo from Office of

Management and Budget that put DNSSEC initiatives in writing and made it a requirement, as a major success in this technology area.

Dr. Maughan informed participants that while the DNS work was viewed as a success, similar initiatives to secure BGP were not viewed as positively. Efforts to ensure secure BGP were undertaken through Secure Protocols for the Routing Infrastructure (SPRI) project, but despite these activities, numerous attacks continue. Other factors identified in the inability to secure BGP, included intrinsic difficulties in adding security to established infrastructure protocols and determination of the actual "end customer" (e.g., Internet service providers, routing vendors, network engineers). He noted that SPRI will be working with the American Registry for Internet Numbers to "clean up" existing database and legacy address space problems. SPRI also plans to deploy public key infrastructure solutions between Internet naming authorities and registries and between registries and customers/service providers. Through SPRI, the S&T Directorate will also hold routing security R&D workshops for relevant parties.

Dr. Maughan noted that there was an insufficient deployment of security infrastructure technologies to protect the nation's vital infrastructures due in part to the lack of an experimental infrastructure and rigorous testing and development methodologies. He highlighted the need for the Directorate to understand how infrastructure security research is conducted and what tools are needed to complete the work. As a result, S&T developed the DHS and National Science Foundation Cyber Security Testbed to create a researcher/vendor-neutral environment to produce rigorous testing frameworks for next-generation cyber defense technologies. He identified the inability to access data as another concern that the agency is addressing through the development of the Protected Repository for Defense of Infrastructure against Cyber Threats (PREDICT). PREDICT is a data portal intended to advance the state of R&D efforts on network security products resulting in defensive cyber security technology improvements.

Dr. Maughan reviewed the DHS Cyber Security R&D program, another effort focused on encouraging development of cyber security technologies. To address this critical area of focus, DHS S&T issues broad agency announcements (BAA) to: (1) perform R&D for improving the security of existing deployed technologies; (2) develop new and enhanced technologies for detection and prevention of, and response to cyber attacks; and (3) facilitate the transfer of these technologies into the national infrastructure. The BAA proposals focus on specific technical topic areas, including system security engineering, security of operational systems, and investigative and prevention technologies, and are classified based on the associated stage of technology deployment (i.e., new, prototype, or mature). New technical topic areas such as botnets and other malware, cyber security metrics, network data visualization for information assurance, and Internet tomography/topography were issued in the new solicitation for proposals.

DHS is conducting research in many areas relevant to the discussions of the RDX Workshop, including Internet mapping, routing security management, and visualization tools for network analysis. S&T is involved with cyber security R&D efforts such as small business innovative research and the Rapid Technology Application Program. These programs have conducted research into topics such as crossdomain attack correlation technologies, realtime malicious code detection, botnet detection and mitigation, and exercise scenario modeling. Dr. Maughan identified three emerging technology areas that S&T is pursuing: (1) virtual machine environment – detection and escape prevention; (2) next generation crimeware defenses; and (3) botnet command and control detection and mitigation. The agency has increased its effort to reach out to commercial entities with initiatives like the System Integrator Forum and Cyber Entrepreneurs Workshop. These events cultivate public-private relationships to help both groups achieve their goals of developing and deploying technologies to secure the critical infrastructure.

In summary, Dr. Maughan emphasized that while DHS faces some difficulties in completing its mission, it has made significant improvements. He noted that

the approach to addressing cybersecurity challenges is changing because of more overall awareness and attention to the issue and the development of new public-private partnerships. He stated that DHS S&T is pursuing an aggressive cyber security research agenda in close coordination with industry and academia to improve research tools and datasets and to solve current and future cybersecurity challenges.

2.9 Presentation – Dr. Chris Greer

Mr. Copeland introduced Dr. Chris Greer, Director, National Coordination Office for Networking and Information Technology Research and Development (NITRD). Dr. Greer thanked the NSTAC Industry Executive Subcommittee for the opportunity to present and thanked Motorola for hosting this year's RDX Workshop. He then referenced the *Federal Plan for Cyber Security and Information Assurance Research and Development* to emphasize the importance of the information technology (IT) infrastructure to global public and private sector activities. He stated that safeguarding the IT and critical infrastructure is a matter of national and homeland security.

Dr. Greer provided an overview of the NITRD program, which was established about 17 years ago and has its legislative basis in the *High-Performance Computing Act of 1991* and the *Next Generation Internet Research Act of 1998,* and the *America COMPETES Act of 2007.* The program has a number of responsibilities including: (1) improved security for computing and networking systems in Federal and other realms; (2) long-term basic and applied research on highperformance computing, network systems, and related software; and (3) education and training in software engineering, computer science, cyber security, applied mathematics, library and information science, and computational science. NITRD's mission is to empower individuals and organizations, promote innovation and progress, provide for security, and improve the quality of life by accelerating R&D and educational advances in networking and information technologies through coordination, joint planning, partnerships, and information sharing across Government, academic, nonprofit, and commercial sectors, national and international.

Within the structure of the Executive Office of the President, the NITRD Subcommittee reports directly to OSTP and includes participation from a number of Federal agencies in order to create synergy and reduce redundant efforts. The program has an extensive budget that has seen continuous growth over the past four years. The President's Council of Advisors on Science and Technology (PCAST) enables the President to receive advice from the private sector and academic community on science and technology research priorities and is composed of appointed individuals from various industry, education, and research entities. PCAST conducted a 2007 assessment of NITRD, which found that the program effectively balanced its mandates and mission requirements, but the current coordination processes were inadequate to meet national needs. The assessment recommended that the NITRD Subcommittee develop and maintain a strategic plan and public technology R&D plans. As a result, the NITRD program issued a request for input in order to get ideas on possible areas of focus.

Dr. Greer explained that cyber security and information assurance (CSIA) is a critical research area that originated from a PCAST recommendation in the assessment report which stated that the Interagency Working Group on Critical Information Infrastructure Protection should be the focal point for coordinating Federal cyber security R&D efforts and should be integrated under the NITRD program. CSIA addresses the security of computer-based systems that support critical infrastructures and other vital Federal missions, and coordinates close communication and liaison among the CSIA agencies, academia, and industry to address CSIA R&D needs. CSIA has representatives from many of the Federal organizations that participate in NITRD.

Dr. Greer mentioned the National Intelligence Council's 2002 report titled "Mapping the Global Future" in order to highlight the need to develop "game-changing" approaches to responding to critical infrastructure threats. He then summarized some of the key R&D coordination and leapahead activities being developed under the CNCI. The CNCI vision for R&D is to develop a high-priority and coordinated set of Federal activities

to transform the cyber infrastructure to protect national interests. The CNCI identified several principles for multidimensional cyber R&D; three of which were highlighted by Dr. Greer: (1) improve synergy between classified and unclassified Federal research; (2) enable a broad multidisciplinary, multi-sector effort; and (3) exploit the full range of existing R&D models and develop new, streamlined approaches for high-risk and high-payoff R&D. NITRD will serve as the foundation for CNCI's coordination activities because of the program's history in research coordination and familiarity with NITRD participants who have science and technology expertise.

In closing, Dr. Greer underscored the importance of public-private partnership in the effort to implement the CNCI and the Federal strategy to secure cyberspace. He asked Workshop participants to discuss their ideas within the context of the need for more public-private partnerships.

3 Breakout Sessions

Mr. Copeland described the breakout session topics and introduced the facilitators who would be leading those sessions. The session topics, facilitators, and staff support are listed below.

Over the course of the two days, participants met with their breakout session groups to closely examine a particular issue area and identify the key priorities for further study. To facilitate the discussion of research and development (R&D) needs associated with evolving national security and emergency preparedness (NS/EP) communications in the global environment, moderators asked participants to consider the following questions:

- Which aspects of R&D initiatives that are underway require additional coordination?
- What current activities address the issue and how can they improve NS/EP communications?
- What impediments might inhibit further R&D?

Breakout Session	Facilitators/Staff
Emergency Communications Response Networks	Ms. Peggy Matson, Motorola Mr. Dan Phythyon, Department of Homeland Security Mr. Scott Booth, Booz Allen
Convergent Technologies	Mr. Patrick Beggs, DHS Mr. Jim Mathis, Motorola Mr. Dawane Young, Booz Allen
Defending Cyberspace	Mr. Robert Dix, Juniper Networks Mr. Robert Leafloor, Industry Canada Ms. Sarah Greenwood, Booz Allen
Identity Management	Mr. James Zok, CSC Mr. Tony Rutkowski, VeriSign Mr. Perry Fergus, Booz Allen
Emerging Technologies	Mr. Siafa Sherman, Nortel Networks Ms. Elizabeth Hart, Booz Allen Ms. Avonne Bell, Booz Allen

- Based on the session discussions, what input would you provide to a research agenda and budget requests? What are the underlying policy issues that should be studied by the NSTAC or international counterparts?

- What would be your three to four key points related to developing an agenda for action on R&D efforts as related to this particular topic?

In addition to addressing and expanding on these questions, breakout session groups introduced other discussion items of particular relevance to their topic area. Observations and results from the breakout sessions follow. The different breakout session groups were encouraged to identify key areas of concern and possible solutions or ways for addressing the problem. The information below represents the discussions, ideas and final thoughts of the 2008 Research and Development Exchange (RDX) Workshop attendees but the suggestions provided herein are not consensus and are not an official position of the President's National Security Telecommunications Advisory Committee (NSTAC), the R & D Task Force or its members.

3.1 Emergency Communications Response Networks

Participants focused on the need for R&D that would address the numerous challenges facing emergency communications. The group discussed the vision for emergency communications from a technology perspective and identified five overarching fundamentals that should guide emergency communications R&D efforts: (1) the emergency response community should be involved in all R&D and related policy initiatives, supported by industry and academia; (2) business cases are needed to ensure sufficient funding is aligned to emergency communications R&D; (3) technologies should be developed and deployed in a way that results in a graceful migration and leverages existing investments and resources (e.g., infrastructure, spectrum) to the greatest extent possible; (4) requirements being addressed must be consistent with the mission need; and (5) R&D efforts should be aligned with and support the National Emergency Communications Plan (NECP).

3.1.1 The Current Landscape

When considering the current emergency communications R&D landscape, participants noted that current efforts are being driven by the Department of Homeland security and being coordinated among Government, industry, and academia to varying degrees. The group agreed that these efforts are necessary, but not sufficient for achieving the desired end state. the group focused the discussion on technology development, standards development, and testing initiatives, many of which centered on improving interoperability among emergency response providers. While participants noted that many efforts exist, specific topics and related initiatives discussed included:

- **Multi-band Radio and Antenna:** enables responders to communicate across multiple frequency bands using a single device.

- **Common Air Interface and Inter Sub-System Interface:** development open architecture standards for interoperability.

- **Compliance Assessment Program:** establishing a testbed to validate Telecommunications Industry Association/Electronics Industry Association-102 (Project 25) compliance of vendor products.

- **National Visualization and Analytics Center:** developing algorithms through six university centers focused on interpreting event information for decision making purposes.

- **Protection of Wireless Networks:** testing the security of digital transmissions.

Participants focused on the need for R&D to address the numerous challenges facing emergency communications. The group set the direction for the work to follow by agreeing on a desired end state. The discussion centered on the activities and changes required to achieve this desired end state. The desired end state was described as having three core elements:

- **Operability and Interoperability**
  - Secure interoperability across wireless networks with disparate protocols and frequency bands, including both private and public networks and legacy and next generation technologies, without restricting mobility
  - Ability to share media among Government agencies, the general public (e.g. alerts, pictures), and operators of critical infrastructure
  - Ready access to reliable communications for disaster response, including supplemental communications capabilities (e.g., satellite, rapidly deployable capabilities), communications that operate in starved environments (e.g., alternative energy), and capabilities that can be relocated (e.g., Next Generation E911)
  - Primary communications capabilities that are built to withstand the physical punishment and heavy call load of a major disaster
- **Spectrum**
  - The ability to fully utilize spectrum best suited for the task, including the opportunistic use of secondary use spectrum (e.g. television white space) and unlicensed spectrum
- **Access to Tailored Intelligence**
  - Access to and consolidation of volumes of all-media data to create easily consumable, user-tailored intelligence. The presentation of such intelligence should enable a highly informed and timely incident response (e.g., high velocity human factors)

3.1.2 Challenges and Impediments

The group agreed on key challenges and impediments to emerging technology R&D efforts that should be prioritized moving forward. The group recognized that any emergency communications R&D efforts could be hindered by the lack of well-defined and validated requirements, the ability to justify R&D investment by industry based solely on public safety requirements, budgetary constraints, and the lack of training and operational protocols to accompany new technologies or solutions. Further, participants indicated that the policy impacts of technology must be considered throughout the R&D process, noting that existing policies should be evaluated as new technologies become available. The participants further discussed specific challenges in each of the three overarching areas.

- **Operability and Interoperability:** Participants agreed that improving the mobility of emergency response providers would require close collaboration between the emergency response community, industry, and academia. The group noted that mobility requirements would need to be aggregated across the emergency response community to create a viable business case for industry investment, as most current solutions are not sufficiently affordable. Participants also suggested that close coordination with industry is needed related to the prioritized access to commercial communications capabilities (e.g., public cellular, satellite communications) during public safety or national security events.
- From a security perspective, participants indicated that greater understanding is needed around the security impacts of existing and new technologies (e.g., cognitive radio) in an emergency response environment prior to their release and use. Further, the group identified the need to determine the impacts of new technologies on privacy and the impact of privacy rules on the application of potentially essential technologies.
- **Spectrum Flexibility:** Participants stressed that spectrum should be better aligned to optimize and fully utilize spectrum based on the task being performed, including the opportunistic use of secondary use spectrum (e.g. television white space) and unlicensed spectrum. Participants also discussed the need to better define how broadband will be used in an emergency response environment. An understanding of the requirements for broadband will better position emergency responders to take advantage of additional spectrum as it becomes available.

- **Access to Tailored Intelligence:** The group noted that the consolidation and standardization (i.e., data exchange) of volumes of media data is needed to create the easily consumable, user-tailored intelligence to enable incident response. The ability to share and present this information effectively was also considered important to establishing command and control, as well as event situational awareness.

3.1.3 The Path Forward

Based on the discussions, participants noted that future emergency communications R&D priorities should address the following key priorities. Additional priorities identified by the group are in Appendix D.

Operability and Interoperability

- **Develop a universal handheld device that enables mobility and roaming across systems.** Participants recognized the importance of mobility and the ability for public safety users to roam across disparate systems (i.e., public and private) to support both local and regional incident response. The group noted the importance of ensuring such a capability is aligned to user requirements. In addition, technology to support such a device must address security as users roam across systems, including authentication methods for both the user and device. Participants also noted that the device must be affordable to ensure adoption by the public safety community.

- **Establish a viable industry business case for technologies tailored to support NS/EP communications.** Participants agreed that Government and industry should work together to establish a viable industry business case for the development of technologies to support NS/EP communications. To help justify industry investment in R&D, emergency responders across all levels of Government (i.e., Federal, State, local, tribal) should establish a common set of strategic user requirements (e.g., infrastructure sustainability) that broadens the potential market for future technology. Participants agreed that where mission critical requirements exist and a viable business case does not, the Federal Government should identify opportunities to defray industry risk and investment through existing or new Federal R&D programs.

- **Availability of priority services and enabling technologies.** The participants recognized the importance of industry and Government collaboration to ensure the availability of secure priority services for NS/EP communications during a significant event. In addition, associated technologies and solutions should address requirements such as authentication, end-to-end security, and quality of service.

- **Establish security testbeds to evaluate technologies that support NS/EP communications.** Participants recognized the importance of understanding the security impacts of existing and new technologies in an emergency response environment. The group agreed that security testbeds should be established to determine potential vulnerabilities and risks prior to adoption and use by the NS/EP user community. Participants recommended that security testbeds should be established in both laboratory and field (e.g., pilot) environments to enable evaluation during emergency response scenarios.

Spectrum Flexibility

- **Enable the cognitive use of spectrum.** The participants agreed that further R&D is needed for technologies that optimize the use of spectrum to support NS/EP communications. Specifically, the group noted that further R&D is needed for the cognitive use of spectrum for NS/EP. Areas identified for further investigation included security, interference, sensing technologies, identity management, and priority management.

Access to Tailored Intelligence

- **Enhance command, coordination, and situational awareness capabilities.** Participants agreed that improved capabilities are needed to support command and coordination, and situational awareness during emergency response missions.

Specifically, participants noted that further R&D is needed to adapt and demonstrate the viability of capabilities such as video analytics, sensors, and bio-monitoring in an emergency response environment. For example, participants discussed the need to develop methods to synthesize bio-monitoring information that provide an indication of emergency responder health and safety.

Recognizing the strong role that policy will play in facilitating the establishment of enhanced emergency communications capabilities, participants also recommended that specific policy initiatives should be established, including:

- Develop a policy architecture to enable roaming and technology to help execute policy;
- Develop the impact of new technologies on privacy and the impact of privacy rules on the application of potentially essential technologies;
- Determine the policy impacts of preemption of new mobility model;
- Determine how spectrum policies can be optimized for increased flexibility and sharing across levels of Government; and
- Determine requirements for situational awareness content by emergency response function.

Additional policy initiatives identified by the group are shown in Appendix D.

The following table (Figure 1) clarifies the agenda for action discussed during the Emergency Communications Response Networks breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

3.2 Convergent Technologies

Convergent technologies—the use and combination of existing technologies to create new products and services—are increasingly being utilized by NS/EP

Research Area	Suggested Focus
Develop a universal handheld device that enables mobility and roaming across systems	▶ Mobility and the ability for public safety users to roam across disparate systems are important to support local and regional incident response ▶ Technology to support this device should take security concerns of operating across systems into account
Establish a viable industry business case	▶ Establish a viable industry business case for the development of technologies to support NS/EP communications ▶ Establish a common set of strategic emergency responder user requirements that broadens the potential market for future technology
Ensure availability of priority services and enabling technologies	▶ Ensure the availability of priority services for NS/EP communications during a significant event
Establish security testbeds to evaluate technologies that support NS/EP communications	▶ Establish security testbeds to determine potential security vulnerabilities and risks prior to the adoption of existing and new technologies for use by the NS/EP user community
Enable the cognitive use of spectrum	▶ Conduct further R&D regarding security, interference, sensing technologies, identity management, and priority management
Enhance command, coordination, and situational awareness capabilities	▶ Conduct further R&D to adapt and demonstrate the viability of capabilities such as video analytics, sensors, and bio-monitoring in an emergency response environment

Figure 1 Emergency Communications Response Networks Agenda for Action

Current Convergent R & D	
▶ IETF Working Groups- Pre-congestion Notification ▶ Next Generation Internet – Qbone Premium Service (QPS) ▶ DNSSEC, BGP security, DETER testbed ▶ DSN (Defense Switched Network) Assured Services Research	▶ Internet Research Task Force – Internet Congestion Control and IP Mobility Optimization (MOBOPTS) ▶ GEANT & GEANT2 projects ▶ GENI and FIND ▶ NCS TIB 05-01" VoIP/E-9-1-1 for NS/EP ▶ NCS Modeling and Simulation Research
Convergent Key Technologies and Academic Areas of Focus	
▶ Mitigation of degraded network environment ▶ Prioritization of Applications and Services* ▶ Development of Mesh Ad hoc / Cognitive Network Elements Addressing the limitations of Internet Protocol (IP) ** Identified by participants as a high priority item*	▶ Creating authentication and priority at Layer 1 and Layer 2 of the OSI model ▶ Configuring or developing network elements that consume less power ▶ Creation of Forensics tools in a converged network environment to analyze network attacks

Figure 2 Current Convergent R&D Activities and Key Technology Areas

users. Convergent technologies bring combinations of video, traditional voice, Internet, and wireless services onto one platform that is seamless to users. Participants noted the significant increased utilization of convergent technologies to deliver enhanced NS/EP communications. Fundamental technology standards and regulatory issues need to be the focus of convergent technologies R&D initiatives.

3.2.1 The Current Landscape

Participants identified numerous current convergent R&D activities and technology areas (Figure 2), but focused the discussions on three major areas shaping the current convergent technologies landscape.

- **Application and Service Prioritization:** Participants analyzed the emergency response community's use of convergent technologies. Participants discussed the increased reliance by first responders on technologies such as wireless, Internet browsing, e-mail, text messaging, streaming video, file sharing, satellite communications, and the global positioning system during national emergencies. These applications and services traverse fixed bandwidth networks. Thus, during national emergencies that cause networks to have limited bandwidth, applications and services that are more critical than others may not be functional due to usage by less critical applications and services. Public service agencies rely on applications being provided by third parties and hosting companies. Currently, there is no framework for prioritizing the usage of the applications provided by these services.

- **Cyber Crime Scene Investigations:** Participants identified security as a fundamental issue regarding convergent technologies. Participants noted the need for forensics tools to analyze network attacks in a converged network environment. There are significant and inherent differences between the current network security environment and the future network environment which will be heavily composed of convergent technology network elements. As new technologies and user devices begin to interface with the network, additional threats and vulnerabilities become more prevalent.

- **Alternative Energy Solutions:** Participants also described the important relationship between power and communications. One member emphasized the need to deploy network elements and user devices that utilize and consume smaller amounts of power. The group also discussed strategies for network elements to avoid network outages due to loss of power. Significant R&D

efforts in alternative sources of energy and conservation of power are underway. The examples the participants noted were the possible use of solar, wind or bio-diesel fuels during network events. Participants agreed that establishment of a well-defined energy conservation strategy involving relevant stakeholders is critical to accelerate the convergence of the gains made in alternative energy with those of convergent technologies.

3.2.2 Impediments and Challenges

Participants identified three overarching impediments to increased convergent technology R&D.

- **Network Availability:** Participants recognized that the increased use of convergent technology brings new challenges, particularly in limited network availability or constrained bandwidth situations. Participants agreed that decisions related to access control and application availability are key issues in this area.

- **Network Security:** To further identify shortfalls of convergent technologies, participants raised several areas of concern around the ability to provide network security at layer 1 and layer 2 of the Open Systems Interconnection (OSI) model. The ability to authenticate users and network elements to differentiate bad actors from authorized users is important. Several participants emphasized the criticality of ensuring network security at the transport layer based on the significant threat posed at this level.

- **Driving the Business Case for Key Stakeholders:** Participants identified the need for the Federal Government to provide incentive to key stakeholders to make the necessary resource and infrastructure changes to their networks in order to make networks effective for NS/EP use. Participants noted the challenge of getting businesses to act without clear economic incentives for stakeholders.

- **International R&D Coordination:** Participants noted that some domestic traffic traverses networks outside of the United States. One member illustrated how domestic users can be routed through Asia to reach websites in the United States. Therefore, international coordination and standards creation to address NS/EP communications needs is imperative. Group participants agreed that ongoing international R&D activities are not well coordinated. Participants suggested that increased cross-border coordination of ongoing R&D activities is warranted to better leverage available R&D resources and ensure adoption of effective protocols. Participants noted the challenges of having a lack of mechanisms to determine international, national, and local agreements around NS/EP communications.

3.2.3 The Path Forward

In evaluating key drivers toward enhanced convergent technology deployment and use, the session participants identified three prioritized R&D areas that deserve critical attention:

- **Create a roadmap for evolving NS/EP communications in a converged technology environment.** Participants concluded that there needs to be a comprehensive framework that outlines the path forward for incorporating convergent technologies into next generation networks (NGN) to ensure effective NS/EP communications in the event of a national event. In order to develop the framework, the minimum technology requirements for NS/EP users and first responders need to be identified. Additionally, participants emphasized the need to develop standards and technology requirements to ensure systems work properly regardless of bandwidth limitations to ensure priority within network elements. Finally, participants noted the need to develop a policy framework to ensure service providers have the ability to provide priority services, and are not constrained by existing policies and regulations.

- **Further development of modeling and simulation, forensics, and trusted relationship constructs during NS/EP events.** Participants emphasized the need for collaborative mechanisms to enable more effective information sharing, coordination, and progress in the area of forensics, modeling and simulation, and authentication. Participants identified the need

for R&D investment in the area of applications that address monitoring mechanisms to establish adequate controls.

- **Initiate research to develop and deploy network elements that more rapidly reconstitute and use alternative power sources in the event of a national emergency.** Participants emphasized the significant potential of alternative energy sources that combine R&D of the alternative energy sector and the convergent technology sector. Participants further noted the need to create communications systems that are interoperable with alternative power sources. Participants acknowledged that network elements that require less power are more likely to maintain the ability to operate in a limited power network event situation.

The table below (Figure 3) clarifies the agenda for action discussed during the Convergent Technologies breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

3.3 Defending Cyberspace

Participants engaged in a broad discussion concerning a variety of issues related to defending cyberspace. The dialogue covered everything from the definition of cyberspace to risk management to attribution to economic justification, all within the context of industry and Government collaboration. The group emphasized, among other things, the need for a comprehensive inventory or database of current and past Government and industry cybersecurity R&D available to all stakeholders. The group also recognized the need for an environment in which Government, industry, and academia can share R&D information and provide a unified front on the issue of defending cyberspace.

3.3.1 The Current Landscape

The task of defending cyberspace is far from simple. Participants agreed that there is insufficient actionable information about threats; an incomplete understanding of network, software, and hardware vulnerabilities; and an inadequate appreciation for the potential consequences of a cyber attack. They also agreed that there is significant room for improvement in industryGovernment collaboration on cyber defense; when executed effectively, these publicprivate partnerships can attempt to close these information gaps and better defend our cyber landscape.

The group identified three areas shaping the current landscape with regard to defending cyberspace:

- **R&D Inventory and Evaluation:** The current environment lacks a comprehensive inventory of cybersecurity R&D conducted by both industry and Government that is available to all stakeholders.

Research Area	Suggested Focus
Create (1) a roadmap for the minimum requirements for services and applications for NS/EP users and first responders and (2) a prioritization framework for applications	▶ Identify technology requirements of first responders ▶ Create a critical application matrix and threat vulnerability assessment ▶ Develop standards and technology requirements and a policy framework to ensure proper provider response in an NS/EP situation
Further develop modeling and simulation, forensics, and trusted relationship constructs during NS/EP events	▶ Focus research and development efforts on: (1) applications that provide analysis of cyber attacks; (2) approaches to increase the ability of multi-layer systems to provide authentication at all layers; and (3) modeling and simulation mechanisms to determine threat vectors
Initiate research to develop and deploy network elements that more rapidly reconstitute and use alternative power sources in the event of a national emergency	▶ Create communications system interoperability with alternative power sources ▶ Develop network elements that require less power and have the ability to operate in a limited power network event situation

Figure 3 Convergent Technologies Agenda for Action

This gap, combined with a lack of metrics to measure the value of previous R&D investments, leaves today's cybersecurity teams with an incomplete picture of the current landscape. Participants expressed concerns not only about unnecessarily duplicating R&D, but also about being unaware of how past efforts have, or have not, made cyberspace safer and more secure.

- **End User:** Participants identified the end user as a fundamental player affecting cyber defense today. One participant suggested that despite all of the identified and yet-to-be discovered vulnerabilities in software and hardware, users themselves are the biggest vulnerability to the cyber network. The responsibility for defending cyberspace is being inadvertently pushed to the end user who may not be capable of installing and maintaining the tools necessary to protect his or her machine from attack. Participants discussed options such as distributed security or "invisible" security built into software and hardware. Security needs to be user friendly and easy-to-understand, and it should enable instead of burden the end user, especially secure NS/EP users. It was suggested that end users should take a stand and insist that industry provide these types of security tools; the increased demand could provide the much needed economic justification for many commercial firms to invest in cyber defense.

- **Awareness:** The group acknowledged that today's environment is being shaped by a lack of awareness about cyber threats and a sense of apathy toward cybersecurity in general. A participant suggested that to this point, there has not been a significant enough collapse of U.S. infrastructure due to a cyber attack to trigger a public outcry or to prompt action.

3.3.2 Challenges and Impediments

The breakout session group identified five major impediments and challenges to future R&D efforts in advancing cyber defense:

- **Privacy:** Participants agreed that privacy protection is, and will continue to be, a challenge for cybersecurity R&D. Efforts to monitor Internet traffic in order to detect malicious behavior or hacker practice runs could attract criticism from such organizations as the American Civil Liberties Union. The participants also discussed the complications that Voice over Internet Protocol (VoIP) brings to existing monitoring efforts; specifically, they addressed the issue of whether or not the capture of IP data that by chance contains VoIP data would be considered wiretapping. The group noted that future R&D efforts must be conscious of privacy concerns and must seek to strike an acceptable balance between privacy and security.

- **Globalization:** The group noted the varying challenges that globalization poses for cybersecurity. The rapid increase in computer connectivity, the growth in the use of the Internet, and the existence of global network infrastructure increases the number of threats to our Nation's infrastructure as well as further complicates the issue of attribution. Future solutions for defending cyberspace will require not only Government and industry collaboration, but also responses that cross international borders, political divides, and cultural boundaries. Another aspect of globalization that is an impediment to cybersecurity R&D is the reality that industry conducts the design, manufacture, and service of many information technology (IT) products outside the United States. Participants discussed the lack of integrity in supply chain processes; they noted that U.S. buyers may be purchasing from unauthorized foreign sellers and in turn receiving infected hardware or software. The group also expressed concern that with production taking place overseas, U.S. security experts may not understand how components work or how they are coded; they noted that it is difficult to secure something that we do not understand.

- **Business Case:** Group members acknowledged the lack of a strong business case to spur industry to invest in cybersecurity R&D or in the implementation of previously developed solutions. Specifically, the group noted the slow implementation of IP version 6 (IPv6) and Domain Name System Security Extensions due to a lack of incentives for commercial firms. The members also

examined the applicability of risk management as a tool to identify existing cybersecurity gaps, which in turn helps to prioritize future R&D. Participants noted, however, that existing applications of risk management are hampered by a dearth of realistic threat data from the Federal Government to plug into risk calculations.

- **Human Capital:** The computer industry faces a two-fold challenge in the coming years related to human capital. Participants raised concerns about an impending shortage of computer science (CS) and engineering graduates that could impede future R&D efforts. They highlighted the need to not only spark high school and undergraduate student interest in cybersecurity related majors, but also to expand and to diversify existing scholarship programs through industry-Government partnerships. The other issue is that many undergraduate and graduate CS curricula lack depth in security teachings, and the group noted that many textbooks still do not include secure programming techniques. Students need to learn secure programming skills in a controlled environment so they can enter the workforce and immediately contribute to cybersecurity efforts.

- **Classified Nature of Many R&D Efforts:** Though participants understand and respect the necessity of strict classification and compartmentalization, there was widespread perception amongst the group that the classified nature of a large amount of cybersecurity R&D impedes and challenges R&D in general. Participants expressed concerns about unnecessarily duplicating research already taking place in the classified environment. The group also articulated support for establishing a method to evaluate "old" R&D for its applicability to today's network.

3.3.3 The Path Forward

The breakout session group discussion covered a wide variety of topics related to defending cyberspace. Throughout the discussion, participants identified a number of issues, including end user security and human capital that require action on the part of industry and Government or issues that could guide future R&D. Group members, however, recognized the importance of agreeing on a handful of targeted areas for further development. The group identified four specific areas that deserve critical attention in the area of cybersecurity R&D:

- **Develop a bi-directional architecture and system of processes to establish a National Cyberspace Defense System.** Participants engaged in a lengthy discussion around the concept of a national secure domain. Ultimately, the group agreed that research should be conducted to develop a bi-directional architecture and system of processes to establish a National Cyberspace Defense System. This system would defend infrastructure in the United States from attacks such that every node on the network would have assistance in defending itself from cyber attacks, both foreign and domestic. The system would necessarily operate as a collaborative program with industry and would leverage actionable threat information gathered from across industry and Government. The concept as espoused by the participants would include built-in securities that would reduce security responsibilities placed on the end user. The goals of such a system would be to diminish the impact of cyber attacks, to increase the cost for our enemies of conducting an attack, and to accelerate our ability to recover from attacks by enabling containment.

- **Collaborate with behavioral sciences to study development and propagation of malicious code.** Participants suggested that there is a need for collaboration among traditional computing and behavioral and social sciences as it relates to development and propagation of malicious code and activities. The combined spheres of knowledge could attempt to determine what triggers a person to write malware and what are the behaviors throughout the process from idea to design to testing to implementation and finally to upgrades of malware. Together, the fields could foster the development of a model for how a hacker or hacker community cultivates target selection and development as well as motivations, incentives, and risk analyses that drive and affect a hacker's

decision to act or not to act. Participants agreed that efforts to identify sources and to study the life cycles of malware systems based on how malware morphs, grows, spreads, and ultimately disappears could allow cybersecurity to be predictive rather than simply reactive.

- **Investigate why results of past R&D efforts are not widely implemented.** The group acknowledged that a significant problem facing continued cybersecurity developments is that industry and Government are not implementing the results of past R&D efforts. Participants agreed there is a need to investigate why this is the case and to look at how a range of incentives, or the removal of disincentives, could contribute to address this fundamental problem. Connected to this issue are the needs to ascertain the progress of current cyber defense R&D and to develop a complete inventory of current and past R&D efforts to be available for all stakeholders.

- **Examine the value of licensing as a tool to establish a security baseline.** Participants discussed the issue of establishing a cybersecurity baseline for Federal departments and agencies as well as for industry. As an example, the group felt that research be conducted to examine the need for a licensing process for U.S.-based Internet service providers (ISPs) that would require the ISPs to adopt and to maintain cybersecurity practices commensurate with the most relevant risks as communicated by the Government. Establishment of a security baseline would allow for greater accountability; commercial firms as well as departments and agencies could be held responsible for security breaches that resulted from not adhering to baseline standards.

The following table (Figure 4) clarifies the agenda for action discussed during the Defending Cyberspace breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

3.4 Identity Management (IdM)

Participants focused on the need for concerted R&D initiatives that address the challenges of effective IdM for users, providers, devices, and applications in an increasingly varied and complex communications network environment. Although participants acknowledged that technology-focused R&D (e.g., biometrics) is an important way to enhance IdM

Research Area	Suggested Focus
Develop a bi-directional architecture and system of processes to establish a National Cyberspace Defense System	▶ Focus R&D activities on architecture that prevents every node on the network from being left to defend itself; diminishes the consequences of cyber attacks; and increases the cost for our enemies of conducting an attack ▶ Facilitate industry and Government collaboration to achieve this need
Collaborate with behavioral and social science bodies to study development and propagation of malicious code	▶ Facilitate collaboration among traditional computing and behavioral and social sciences ▶ Model hacker behavior to assess motivations and incentives ▶ Model correlation between release of information and hacker response
Investigate why results of past R&D efforts are not widely implemented	▶ Consider how a range of incentives, or the removal of disincentives, could contribute to addressing this fundamental problem ▶ Ascertain the progress of current cyber defense R&D ▶ Develop an inventory of current and past R&D efforts to be available for all stakeholders
Examine the value of licensing as a tool to establish a security baseline	▶ Conduct research to develop a licensing process for U.S.-based Internet service providers that would require them to adopt and to maintain specific cybersecurity practices

Figure 4 Defending Cyberspace Agenda for Action

capabilities, they also emphasized that governance, including policies and organizational mechanisms, and R&D activity coordination are essential to deliver a fully responsive IdM framework that will also support NS/EP-specific IdM requirements.

3.4.1 The Current Landscape

Participants began characterizing the current IdM landscape by briefly reviewing recently published documents, including the 2008 Identity Management Task Force Report of the National Science and Technology Council,related International Telecommunication Union (ITU) standards documents (e.g., paper on capabilities for enhanced global IdM trust and interoperability, NGN IdM framework contribution), as well as the 2006 NSTAC RDX Workshop global-scale IdM breakout session summary. Participants validated select report findings, and emphasized the fundamental need for more reliable and secure IdM capabilities and for clearer policy and strategies that address robust authentication through digital credentialing and enhanced interoperability among and across autonomous authentication systems.

The group noted numerous IdM standards efforts were underway (e.g., ITU, International Standards Organization SC27 and SC37, American National Standards Institute M1, and National Institute of Standards and Technology/Federal Information Processing Standards 201) as well as other public- and private-sector activities/groups with a R&D component, including Liberty Alliance, OASIS, OpenID, CardSpace, Higgins, and Shibboleth initiatives. Discussion also focused on the IdM-specific requirements for NS/EP communications, including supervisory control and data acquisition infrastructure protection needs, IdM specific to an incident response environment, priority access during major emergencies, support for services restoration after major disasters, and security-related service provisioning constraints. The participants also discussed IdM in the context of cybersecurity needs, specifically more effective use of IdM capabilities to enable protection of cyber systems.

The group identified and cataloged multiple ongoing standards and IdM activities and generally agreed on the need for more coordination and alignment across existing activities and better exchange of information, results, and event horizons across all stakeholder communities (e.g., Federal, State, and local governments, academia, research community, and the private sector).

Participants discussed technology areas that would offer the greatest potential to improve IdM for NS/EP communications. Areas identified as "key" included:

- **Biometrics R&D infrastructure** to drive increases in both performance and function;
- **Technologies for establishing interoperability and trust** such as common credentials, ease-of-use features, and capabilities that address IdM beyond individuals' identity (e.g., applications, devices, service providers, identity providers);
- **Federated identity** an approach for developing a common rule set that allow identities issued by different processes and places to be recognized and treated equally;
- **Discovery** of authoritative identity information and identity providers on global-scale; and
- **New scalable/extendible architectures.**

In addition to these items, the group also identified public key infrastructure implementation, the development of "multi-mode" cards (i.e., integration of multiple solutions on a single platform), and IdM of objects and object binding (e.g., location awareness) as technology areas that hold promise for IdM and its application to NS/EP communications.

3.4.2 Impediments and Challenges

Participants identified several overarching issues that currently impede effective IdM development and implementation as well as challenges that may inhibit further R&D for IdM technologies and standards. Key issues and challenges were categorized into four areas:

- **Trust:** Participants discussed the need for effective vetting processes and audit regimes to ensure the validity of credentials. Associated issues include the need for reciprocal trust methods to verify agreements, the ability to tie an individual identity to a device and a device to a provider. Accepted trust models must address authentication requirements and the issue of root identification (e.g., trustworthiness of the original source of identification such as a passport) and must support both user privacy and anonymity features.

- **Technology:** In the technology area, participants agreed that "usability" and ease-of-use features will be a key driver in the adoption and eventual pervasiveness of IdM capabilities. The group also noted that technology R&D initiatives do not necessarily have to "shoot for the moon" in terms of extensive IdM features and functionality and that quicker and wider user acceptance of interim solutions may be preferable to more complete but longer-term solutions. Participants also discussed technology approaches and the cost benefit tradeoffs of IdM features, including context dependent functions, biometrics accuracy and future technology advances, better forensics for verification of identification, and international differences in the pace of technological progress.

- **Social Issues:** Participants identified social issues that should be considered in IdM planning, research, and implementation. First, cultural differences both domestically and internationally likely will affect the level of acceptance and use of IdM features. For example, user perspectives differ widely from country to country regarding definitions and expectations of privacy and acceptable levels of sharing personally identifiable information. The group also discussed "generational" differences in the use and acceptance of technology, the concept of "socialization of control of identity," and the importance of ease-of-use features to drive user acceptance of IdM technology.

- **Policy:** Participants identified several policy-related issues, including the need for mature IdM business models and processes to support pervasive use, international acceptance of IdM standards via federated identities, and a clear delineation of roles, responsibilities, authorities, and jurisdictional boundaries. An authoritative, comprehensive and broadly chartered governance process, managed within the Executive Office of the President and representing all equities and end-user communities, must be established to guide and direct the federal-government-wide IdM enterprise. In so doing, Government may hope to become a model practitioner in this area, influencing civil IdM implementation through experience and demonstrated, measurable benefit to all parties. Participants also agreed that the United States to promote its interests more effectively in standards bodies. During the policy discussions, participants also discussed candidate issues for future NSTAC consideration, including: evaluating the need for new organizational approaches to IdM; identifying incentives for IdM implementation (e.g., public-private partnerships, grants, business cases, tax-based strategies); identifying incentives for academic participation in IdM standards bodies; evaluating the privacy aspects of IdM; evaluating the role of regulation; and studying effective processes for funding organizations to drive IdM R&D (e.g., National Security Agency, National Institute of Standards and Technology).

3.4.3 The Path Forward

To address the numerous challenges and issues discussed, participants identified IdM priorities for R&D: interoperable trust mechanisms (e.g., certification and accreditation processes, standardization of strength of authentication, and vetting processes); non-user-based IdM such as object, device, and application binding; use of other technologies for identification (e.g., radio frequency identification); and discovery (sources of authoritative identity information). In developing an R&D agenda for action, the group recognized that most if not all public infrastructure IdM capabilities have NS/EP implications; as a result, any progress achieved through basic IdM R&D will have a positive commensurate impact on NS/EP-related IdM capabilities. Reflecting guidance received from the RDX plenary presenters to strive to identify R&D

"game changers," participants developed three actions that could drive significant IdM R&D progress. The participants supported the following items

- **Publish a National Security Presidential Directive to create an IdM governance process across the Federal Government that includes all necessary coordination, outreach, Government-industry collaboration activities.** Established governance will provide oversight, identify roles and responsibilities in the area (e.g., delineating inherently governmental versus private-sector IdM functions), drive interoperable infrastructure development, and identify and establish incentives to drive IdM business cases/private sector adoption;

- **In coordination with the Office of Science and Technology Policy (OSTP) issue an Office of Management and Budget (OMB) policy guidance for the next fiscal year which provides incentives for synergistic participation in standards bodies as a stipulation for IdM R&D funding;** and

- **Within the suggested government-wide IdM governance framework , and responsive to such authorities, direct the National Security Agency (NSA) to facilitate the rules and processes for implementing IdM solutions** (at all levels including privacy protection) to drive an effective, common, global, IdM infrastructure and supporting mechanisms for service providers.

The table below (Figure 5) clarifies the agenda for action discussed during the Identity Management breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

3.5 Emerging Technologies

Participants focused on the need for concerted R&D initiatives that would address challenges presented by the rapidly evolving communications environment. The group acknowledged that many emerging technologies introduce new vulnerabilities as well as opportunities to enhance NS/EP communications. Furthermore, the group agreed that there is a need to examine these emerging technologies to determine their potential impact and identify any tools or policies that will address the rising security issues presented by the evolving communications environment.

3.5.1 The Current Landscape

In considering the emerging technologies that may present either challenges or opportunities for issues associated with NS/EP communications, the participants identified numerous technologies and needs including social network technologies, converged IP technologies, cloud computing, and integrated Federal enterprise backbone capabilities. However, the participants agreed to focus the discussions on those technologies that they viewed as true "game changers" and broke the discussion into four overarching technology areas:

Research Area	Suggested Focus
Develop an IdM governance process	Publish a Presidential Directive for the creation of an IdM governance process, with responsibilities to include policy oversight, identification of roles and responsibilities in the area (e.g., delineating inherently governmental versus private-sector IdM functions), interoperable infrastructure development, and establishment of incentives to drive IdM business cases/private sector adoption
Provide incentives for IdM R&D	OSTP and OMB should collaborate to issue a policy guidance for the next fiscal year which would incentivize synergistic participation in standards bodies as a stipulation for IdM R&D funding
Implement rules for efficient IdM implementation	IdM governance framework that directs NSA to establish the rules and processes for implementing IdM solutions (at all levels including privacy protection) to drive an effective, common, global, IdM infrastructure and supporting mechanisms for service providers

Figure 5 Identity Management Agenda for Action

- **Trusted Architecture:** Participants noted that in the current environment, NS/EP users overall have little trust in the security of data transmitted over the communications infrastructure. The growth and emergence of mobile and cloud technologies exacerbates this concern, and lacking trusted architectures, users will likely continue to operate over increasing less secure platforms. Today's products often do not include security considerations in the system development lifecycle, educators do not teach secure coding, and end users often do not properly configure their machines to protect their data. The participants agreed that there is a need for a trusted architecture model that enables secure, reliable, and trusted end-to-end communications, structure, and data in the NS/EP environment. Such a model might enable secure cloud and peer computing; a strong overall security posture; a standard security model with similar benefits to the OSI model; and defined security attributes across all layers.

- **Distributed/Portable Energy Technology:** Participants noted that the success of long-term NS/EP operations is linked to development of distributed/portable energy technologies, including battery, fuel cells, solar cells, and kinetic chargers. For example, the group noted that it is essential that both first responders and soldiers in the battlefield have access to sources of energy to support the mobile communications equipment upon which their lives and the lives of others depend. Furthermore, the energy demand for the communications infrastructure is growing exponentially, and disruptions to the communications infrastructure due to energy loss have the potential to not only impede NS/EP requirements, but to also lead to social breakdown. The group members agreed that communications infrastructure needs to include distributed/portable energy technologies to enable rapid recovery capabilities, sustained communications during an extended crisis, and expedite the delivery and recovery of resources to meet the needs of an impacted community.

- **Assured Attribution:** The participants agreed that in today's environment it is difficult or impossible to assure the attribution of the source of bad actions that disrupt service because of fraud, terrorist activities, nation-state attacks in cyber space, or other malicious behavior. Attribution is a critical national security issue that many people attempt to address today through techniques such as visualization and data mining. However, the group agreed that a true "game changer" for national security communications would be the introduction of assured attribution capabilities. Such capabilities might enable more accurate and rapid attribution, empower end users to know when malicious activity has occurred, and/or serve as a deterrent for some malicious actors.

- **Dynamic Spectrum Access:** The participants discussed the attributes of dynamic spectrum access, which they described as a new technology that promotes efficient and flexible use of spectrum by sensing spectrum availability and assigning spectrum use in real time. This capability will enable integration of wireless and fixed network infrastructure that contain intelligent systems to control spectrum assignments. The participants noted that demand for spectrum is increasing and spectrum is a finite and increasingly scarce resource. Furthermore, the current static spectrum management approach exacerbates the problem of spectrum availability by dedicating frequencies to stovepipe wireless systems. The participants agreed that a mature dynamic spectrum access technology has the potential to increase spectrum availability to accommodate new users, expand network capabilities by providing mobile access to content and providing functionality that currently resides in fixed networks, and improve utilization of spectrum and network resources.

3.5.2 Challenges and Impediments

The group agreed on key challenges and impediments to emerging technology R&D efforts that should be prioritized moving forward. Overall, the group recognized that any collaborative R&D efforts in the future might be impeded by budgetary constraints, lack of executive level sponsorship, and/or intergovernmental governance and policy enforcement. In addition, the participants noted that the Federal

Government has not delegated management of R&D associated with telecommunications capabilities to any single government entity. Therefore, any future R&D would require coordination across the Government. The participants further discussed specific challenges and/or gaps in each of the four overarching subjects.

- **Trusted Architecture:** The participants agreed that the development of a trusted architecture would require collaboration between industry, academia, and Government to ensure that security is embedded in the system development lifecycle. Corporate enterprises would need to achieve a balance between security needs and business and market drivers. Educators would need to incorporate secure coding in instruction materials. The Government would need to ensure that standards and other security requirements are established. The members further noted that such collaboration is further hindered by the proprietary nature of many potential solutions in this area.

- **Distributed/Portable Energy Technology:** The participants identified three challenges and/or gaps associated with distributed/portable energy technology:

  - **Energy Generation:** The group noted that any individual energy generation solutions need to be hybrids of several energy technologies, such as battery, solar, kinetic, and fuel, to provide flexible energy for communications networks. Furthermore, effective and reliable NS/EP communications capabilities require independent energy generation capabilities separate from the electric power grid. Finally, although initiatives are currently underway for watt to megawatt generation, no initiatives currently address milliwatt to watt generation.

  - **Energy/Power Management:** Participants noted effective use of distributed/portable energy technologies requires the development of energy management capabilities for NS/EP communications. Specifically, the Government must be able to manage power to meet continuity of communications needs, sources for a distributed hybrid solution, and ondemand distribution of prioritization of power.

  - **Energy Usage:** Participants agreed that the use of distributed/portable energy technologies in an NS/EP environment requires increased efficiency of infrastructure components, software based energy controls, and intelligent energy management capabilities embedded in devices.

- **Assured Attribution:** The participants suggested that any solution providing assured attribution must have global support and must balance privacy issues. The group further identified current gaps in efforts to combat cyber crime, including immature techniques to support heuristics for accurate data collection and inefficient data mining and visualization due to a lack of sufficient attribution. The participants agreed that assured attribution capabilities could help advance such efforts.

- **Dynamic Spectrum Access:** The participants noted that the implementation of dynamic spectrum access technology would require a paradigm shift in spectrum access techniques and in spectrum management, including processes, regulation, and policy.

3.5.3 The Path Forward/Research Priorities

Based on the discussions, participants noted that future R&D priority should be given to the following:

- **Develop a trusted security model.** The participants agreed that future research is needed to develop a trusted security model that address standards and integration; end devices including silicon-based implementations; communications and data transport; identity management and access controls; data self-protection application and software coding standards for security; and integration of security into systems development lifecycle through training, education, and mandatory certification for critical applications development.

- **Explore energy technologies to support mobile communications technologies.** The group members recognized the need for future research regarding

distributed/portable energy technologies that would enable the telecommunications infrastructure to operate independently of the electric power grid. Such solutions might include self sufficient local energy generation nodes; hybrid, solar, wind, battery, and other technologies; 10X chip power reduction; 10X battery capacity; room temperature super conducting wire; 10X increase in power management; and new research materials for energy.

- **Enhance assured attribution techniques.** The participants agreed on the need for research focused on the enhancement of attribution techniques that support heuristics for accurate data collection and augment data mining and visualization capabilities. The group further noted that any such research would necessitate a consortium effort among industry, Government, and academia to focus on the development of such techniques and to address privacy issues.
- **Mature dynamic spectrum access technology.** The group members recognized that substantial R&D funding is needed to bring dynamic spectrum access technology to maturity. In addition, the successful implementation of such technology would require sponsorship from senior Government leaders and will involve the integration of existing architecture and migration strategy.

The table below (Figure 6) clarifies the agenda for action discussed during the Emerging Technologies breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

3.6 Breakout Session Summary

The following table (Figure 7) summarizes and clarifies several themes that spanned across the issues discussed in the individual breakout sessions.

Research Area	Suggested Focus
Develop a trusted security model	Conduct research to develop a trusted security model that addresses standards and integration
Explore energy technologies to support mobile communications technologies	Investigate distributed/portable energy technologies that enable the telecommunications infrastructure to operate independently of the electric power grid, including local energy generation nodes; hybrid, solar, wind, battery and other technologies
Enhance assured attribution techniques	Focus on the enhancement of attribution techniques that support heuristics for accurate data collection and augment data mining and visualization capabilities
Mature dynamic spectrum access technology	Provide sufficient R&D funding to bring dynamic spectrum access technology to maturity

Figure 6 Emerging Technologies Agenda for Action

	Emergency Communications Response Networks	Convergent Technologies	Defending Cyberspace	Identity Management	Emerging Technologies
Education, Awareness & Training	Outreach and education for system lifecycle planning & technology migration	Need forensics tools to analyze network attacks	Educate and enable end user; evaluate collegiate curriculum for depth of security teachings	Need for more awareness, coordination, and alignment of ongoing IdM standards and R&D work	Need to integrate security into systems development life-cycle through training and education
Economic Justification	Defray risk/ investment where there is no viable business case based on user requirements	Must incentivize industry to implement new secure technologies	Need for business case; determine expenditures based on cost-benefit analysis	Identification of business cases/ models to support pervasive IdM use	Balance between business and security needs for emerging technology investment
Survivability & Resiliency	Need to research and develop survivable , efficient, longer-lasting power sources for emergency use	Develop network elements that require less power or use alternative power sources	Mission assurance translates into resilience	Need for new scalable and extendible architectures (e.g., SOA), better forensics	Need to provide distributed/portable energy technologies to support long-term NS/EP strategies and operations
Mobility & Access	Develop an affordable, mobile device that enables authentication and roaming across systems	Need to determine application access framework during network event	Implications of widespread network access	Context dependency requirements; Technologies for establishing interoperability and trust (common credentials)	Need for a trusted mobile computing platform to support NS/EP needs
Policy Evolutions	Determine the impacts of new technologies on privacy and the impact of privacy rules	Need to resolve policy issues around net neutrality and prioritization	Exploration of setting baseline standards to enhance accountability in cyberspace	Need to address authority and jurisdiction; international acceptance via federated identities and standards	Need for a paradigm shift in spectrum management (i.e., processes, regulation, and policy)
R&D Infrastructure	Establish security testbeds (laboratory and pilots) to evaluate vulnerability of existing and new technologies for public safety	Need R&D efforts to help provide authentication and priority at Layer 1 or Layer 2 of the network	Behavioral science models; tools to identify life cycle of malware systems	Need for incentives/ funding to drive infrastructure development	Need for coordinated R&D efforts across Government, industry, and academia
Information Sharing	Adapt and demonstrate the viability of command and coordination, and situational awareness capabilities (e.g., video analytics, sensors, bio-monitoring) for public safety use	Need mechanisms to determine international / local/ national agreement	Real-time sharing of actionable threat data	Need for interoperable and reciprocal trust mechanisms, vetting processes, audit regimes, C&A	Need to share information regarding emerging technologies across Government, industry, and academia

Figure 7 Summary of Breakout Session Themes Matrix

4 Closing Plenary Session

4.1 Address – Ambassador Richard Russell

Mr. Guy Copeland, CSC, introduced Ambassador Richard Russell, Associate Director and Deputy Director for Technology, Office of Science and Technology Policy (OSTP), Executive Office of the President. Ambassador Russell stated that his remarks would provide an overview of Federal research and development (R&D) funding trends and activities.

Ambassador Russell informed the participants that the President's fiscal year (FY) 2009 budget calls for the vast majority of funds to be spent on mandatory rather than discretionary programs and fifteen percent of the discretionary budget is allotted to R&D activities. For FY 2009, the total Federal R&D budget is $147 billion, an increase of three percent over FY 2008. This increase is not just for defense R&D spending; non-defense R&D allotments have increased six percent. R&D as a whole accounts for one of every seven discretionary dollars spent by the Government, and funding for R&D-related activities is at a record high. Ambassador Russell commented that in the area of R&D, the concern is prioritization of research needs. He explained that R&D as a share of the total discretionary spending has been constant over the past thirty years.

Ambassador Russell stated that basic research is important because it serves as a driver for innovation. He noted that the Federal Government has historically invested in basic research that has led to a number of important technologies. He highlighted the Administration's focus on research through the announcement of the *American Competitiveness Initiative* (ACI), a funding effort to support innovative R&D in areas such as nanotechnology, supercomputing, and alternative energy sources. ACI is based on the idea that the Federal Government should be responsible for funding long-term and high-risk research. It also emphasizes high priority for research in science areas that will enhance long-term global competitiveness of the United States. ACI specifically outlines goals for U.S. cybersecurity research efforts to address "gaps and needs in cybersecurity and information assurance to protect our information technology (IT) dependent economy from both deliberate and unintentional disruption, and to lead the world in intellectual property protection and control." He noted that Networking and Information Technology Research and Development (NITRD) is one of the Federal Government's main programs for conducting research. NITRD success is evident in the significant increase in unclassified networking and IT R&D investments.

Ambassador Russell then discussed the National Nanotechnology Initiative, a premier program launched in 2000 to invest in nanotechnology research that could impact not only IT, but also a number of other areas. He explained that, prior to 2000, this area was generating significant worldwide excitement but the United States was not a significant investor. Nanotechnology has applications for a number of fields including enabling smaller, lighter, and longer-lasting high performance batteries. Ambassador Russell also discussed the importance of identity management (IdM). He referenced the recently released ***National Science and Technology Council Task Force on Identity Management 2008 Report.*** This report was the product of a task force including representatives from a number of Government agencies who spent six months studying the issue. The report found that there is no accepted definition of IdM, that there is a need for Government involvement, and that a consolidated IdM vision will enable consistent application of privacy controls. The report noted that there would be no "one size fits all" approach but that benefits can be achieved from a meta-framework approach that promotes common technical standards.

Ambassador Russell highlighted the Bush Administration's efforts to promote increased universal, affordable access to broadband. He emphasized the importance of ensuring competition by providing consumers access to multiple service providers as well as access to various types of broadband, not just wireline. He cited data from the Federal Communications Commission indicating that broadband lines have increased from under 10 million in 2001 to over 100 million as of June 2007. He stated that increasing the availability of wireless services would stimulate the deployment of broadband throughout America. He noted that the current Administration's

recent spectrum auction was a significant step, which will increase available broadband and stimulate the development of new and innovative services. He ended by highlighting the rise in the number of mobile Internet users across the United States.

4.2 Closing Remarks – Mr. James Madon

Mr. Copeland introduced Mr. James Madon, Director and Deputy Manager, National Communications System (NCS), Department of Homeland Security (DHS). Mr. Madon thanked the NCS staff and thanked the President's National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee (IES) members, especially Mr. Copeland for their efforts in making the two-day workshop a success as well as Mr. Greg Brown and Motorola for hosting the RDX Workshop. He also recognized the international participants.

Mr. Madon highlighted earlier guidance from the RDX Workshop moderators who emphasized the need to change the rules and provide innovative R&D ideas. He stressed the importance of innovation and collaboration in order to secure the Nation's critical infrastructure. He expressed his hope that the breakout session facilitated discussions that led to ideas for inventive approaches to addressing threats.

Mr. Madon acknowledged and expressed appreciation for senior leadership participation in the event from Ambassador Russell, Assistant Secretary Greg Garcia from the DHS, Office of Cyber Security and Communications, Ms. Susan Alexander from the Department of Defense, Networks and Information Integration, and Dr. Veena Rawat from Industry Canada. He articulated his hope that the senior leadership presentations further facilitated consensus building amongst the group.

4.3 Closing Plenary Session Summary

The closing plenary session of the RDX Workshop ended with reports from the facilitators of the five breakout sessions. The plenary session provided the forum for a high-level discussion of the breakout groups' conclusions and eventual agreement on seven themes that spanned across all sessions:

- **Enhanced education, awareness, and training will reduce security risks and vulnerabilities.** Today's communications networks, information systems, and threat environment have evolved dramatically, resulting in the need for more robust education, awareness, and training programs to educate end-users and system developers alike on security risks and potential mitigation strategies. University programs need to enhance curriculum to teach aspiring developers secure coding and other security measures. Furthermore, service providers and manufacturers that provide equipment and services in support of NS/EP communications need to integrate security into systems development life cycles through training and education. R&D bodies, such as industry, academia, and Government, need to work together to build increased awareness, coordination, and alignment of ongoing IdM standards and R&D work. Finally, the user and standards bodies communities need to enhance outreach regarding security precautions to end-users because in today's converged technology environment many diverse devices are accessing the network and much of the responsibility for security and access control resides with the user.

- **Economic justifications and incentives need to drive R&D efforts in the business community.** The private sector often makes R&D decisions based on the perceived return on investment. Without a viable business case based on user requirements and market drivers, corporate entities are unlikely to pursue specific R&D investments. Any deferment of investment in technologies that may advance NS/EP communications by industry inhibits technological progress and in some cases exposes critical infrastructure and key resources to vulnerabilities. It is important for the Federal Government to provide incentives to industry to implement new technologies. An example discussed in the RDX Workshop was the need to identify business cases and models to support pervasive IdM use. Government efforts to encourage industry adoption of specific security methods should consider the business demands of private companies and ensure that

there is a balance between profit expectations and expectations for technology investment.

- **The communications infrastructure must be survivable and resilient during emergency situations.** The collective desired characteristics of a sound emergency communications system are operability, interoperability, reliability, resiliency, redundancy, scalability, security, and efficiency. The development of network elements that require less power or use alternative power sources will increase the survivability and resiliency of networks during emergency situations. Currently, there is a need for new scalable and extendible architectures with better forensics that utilize distributed and portable energy technologies to support long-term NS/EP strategies and operations.

- **Expanded mobile architectures present challenges related to access and trust for NS/EP users.** An expanded mobile architecture where more intelligence and access points reside at the edge of the network is very prevalent in today's wireless infrastructure. Wireless technology companies have developed significant numbers of affordable mobile device that enable authentication and roaming across systems. These advancements inherently produce a more vulnerable system because of the widespread network accesses. Technologies for establishing interoperability and common credentials are critical. In the wireless network environment, there is a need for a trusted mobile computing platform to support NS/EP needs. In addition to this platform, a priority access framework for users and applications also needs to be developed.

- **Evolving policy approaches need to address the impacts of many new technologies on NS/EP communications.** Recent advancements in technology have brought about significant change; as a result, Government may need to update some policies and regulations to keep pace with the evolving landscape. Some specific areas include the need for policy makers to determine the impacts of new technologies on privacy and the impact of privacy rules on NS/EP communications needs. Regulators need to explore setting baseline standards to enhance accountability in cyberspace and to address authority and jurisdiction as well as international acceptance of laws through federated entities and standards bodies. In addition, regulators need to make a paradigm shift in spectrum management and address the processes, regulations, and policies surrounding spectrum allocation and management.

- **Increased investment in R&D infrastructure needs to drive future R&D efforts.** To accomplish the strategies to support evolving NS/EP communications, key stakeholders much establish laboratories and pilot programs that drive new technologies for public safety. Beyond funding, there needs to be coordinated efforts across Government, industry, and academia to meet NS/EP communications challenges. Some examples for research and development projects that need additional funding are research into providing authentication at Layers 2 and 3 of the open system interconnection model, behavioral science models; and additional tools to identify the life cycle of malware systems.

- **Enhanced information sharing needs to occur between industry, Government, and academia on impending threats and existing R&D efforts.** Stakeholders need to have greater agreement and increased collaboration in order to meet the demands of the evolving NS/EP communications environment. The critical challenge is to engage industry, Government, and academia, as well as end-users in exchanging information about existing initiatives and challenges, thus facilitating the development of comprehensive solutions. Each party needs to share information regarding emerging technologies, interoperable and reciprocal trust mechanisms, vetting processes, audit regimes, and the real-time sharing of actionable threat information. This collaboration needs to take place locally, nationally, and internationally for emergency events.

Following the breakout session presentations, Mr. Copeland invited Dr. Rawat, Ms. Alexander, and Ambassador Russell to offer closing remarks.

Dr. Rawat thanked the participants for their efforts in the discussion and reporting their findings. She remarked that the breakout session output was very useful and would be helpful to her department in their efforts to determine where to put future R&D resources.

Mr. Copeland concluded the 2008 RDX Workshop by thanking Motorola and their staff for being excellent hosts and providing excellent support and facilities; the breakout session facilitators for guiding discussion; and the NCS and Booz Allen Hamilton staff for orchestrating another successful event.

Footnotes

1 The International Telecommunication Union (ITU) in X. 1205 uses the term cyber environment instead of cyberspace to refer to "users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks." For the purposes of this document cyberspace is equivalent to cyber environment.

Agenda

2008 Research and Development Exchange Workshop

Evolving National Security and Emergency Preparedness Communications in a Global Environment

Day 1: Wednesday, September 24, 2008

4:00 – 6:00	***p.m.***	***Preliminary Registration (Motorola Lobby)***
6:00 – 8:00	*p.m.*	*Dinner Reception (Motorola Innovation Center)*

Day 2: Thursday, September 25, 2008

7:00 – 8:00	***a.m.***	***Registration/Continental Breakfast (Motorola Innovation Center Mezzanine)***
8:00 – 11:55	***a.m.***	***Opening Plenary Session (Motorola Innovation Center Auditorium)***
8:00 – 9:45	a.m.	Welcome/Introduction and Speeches
8:00 – 8:05	a.m.	Welcome/Introduction – Mr. Guy Copeland, Vice President of Information Infrastructure Advisory Programs, Computer Sciences Corporation (CSC) and Chair of the Research and Development (R&D) Task Force of the President's National Security Telecommunications Advisory Committee (NSTAC)
8:05 – 8:10	a.m.	Welcome/Introduction – Mr. Greg Brown, President and Chief Executive Officer, Motorola, Inc.
8:10 – 8:30	a.m.	Welcome/Introduction – Mr. Gary Grube, Senior Fellow, Government and Public Safety, Motorola, Inc.
8:30 – 8:50	a.m.	Workshop Overview and Goals – Mr. Copeland
8:50 – 8:55	a.m.	Introduction of Ms. Susan Alexander, Chief Technology Officer, Information and Identity Assurance Office of the Assistant Secretary of Defense (OASD), Networks and Information Integration (NII)/Department of Defense, Chief Information Officer (DOD-CIO) – Mr. Copeland
8:55 – 9:15	a.m.	Moderator's Address from Ms. Alexander
9:15 – 9:20	a.m.	Introduction of Dr. Veena Rawat, President of the Communications Research Centre Canada (CRC), Industry Canada – Mr. Copeland
9:20 – 9:40	a.m.	Address from Dr. Rawat
9:40 – 10:00	a.m.	Coffee Break
10:00 – 10:05	a.m.	Introduction of Mr. Gregory T. (Greg) Garcia, Assistant Secretary for Cybersecurity and Communications, DHS – Mr. Copeland
10:05 – 10:25	a.m.	Moderator's Address from Assistant Secretary Garcia
10:25 – 10:30	a.m.	Introduction of Ms. Leslie Ann Sibick, Chief, Research and Development Analysis/National Infrastructure Simulation and Analysis Center, Office of Infrastructure Protection, DHS – Mr. Copeland

10:30 – 10:50	a.m.	Presentation – Ms. Sibick
10:50 – 10:55	a.m.	Introduction of Dr. Douglas Maughan, Program Manager for Cyber Security R&D, Science and Technology Directorate, DHS – Mr. Copeland
10:55 – 11:15	a.m.	Presentation – Dr. Maughan
11:15 – 11:20	a.m.	Introduction of Dr. Chris Greer, Director, National Coordination Office for Networking and Information Technology Research and Development (NCO/NITRD) – Mr. Copeland
11:20 – 11:40	a.m.	Presentation – Dr. Greer
11:40 – 11:55	a.m.	Introduction of Breakout Sessions & Concluding Remarks – Mr. Copeland
12:00 – 1:00	***p.m.***	***Lunch (Motorola Innovation Center)***
1:00 – 5:00	***p.m.***	***Breakout Sessions***

- Emergency Communications Response Networks
- Convergent Technologies
- Defending Cyberspace
- Identity Management
- Emerging Technologies

Day 3: Friday, September 26, 2008

7:30 – 8:30	***a.m.***	***Registration/Continental Breakfast (Motorola Innovation Center Mezzanine)***
8:30 – 11:25	***a.m.***	***Breakout Sessions (Motorola Conference Rooms – Customer Briefing Center)***

- Emergency Communications Response Networks
- Convergent Technologies
- Defending Cyberspace
- Identity Management
- Emerging Technologies

10:00 – 10:20	a.m.	Coffee Break
11:25 – 12:00	***p.m.***	***Morning Plenary Session (Motorola Innovation Center Auditorium)***
11:25 – 11:30	a.m.	Introduction of Ambassador Richard Russell, Associate Director and Deputy Director for Technology, Office of Science and Technology Policy (OSTP), Executive Office of the President – Mr. Copeland
11:30 – 12:00	p.m.	Remarks by Ambassador Russell
12:00 – 12:45	***p.m.***	***Lunch (Motorola Innovation Center)***
1:00 – 3:05	***p.m.***	***Closing Plenary Session (Motorola Innovation Center Auditorium)***
1:00 – 1:05	p.m.	Introduction of Mr. James Madon, Director and Deputy Manager, National Communications System, DHS – Mr. Copeland

1:05 – 1:15	p.m.	Closing Remarks by Mr. Madon
1:15 – 2:45	p.m.	Breakout Session Facilitator Reports
2:45 – 3:00	p.m.	Plenary Closing Remarks
3:00 – 3:05	p.m.	Workshop Closing Remarks – Mr. Copeland

Attendees

Attendees

Michael Alagna
Motorola, Incorporated

Scott Algeier
Information Technology Information Sharing and Analysis Center

David Barron
Adams and Reese LLP

James Bean
Verizon Communications, Incorporated

Patrick Beggs
National Cyber Security Division, Department of Homeland Security

Avonne Bell
Booz Allen Hamilton

Kathleen Blasco
National Communications System, Department of Homeland Security

Scott Booth
Booz Allen Hamilton

David Boyd
Office of Science and Technology, Department of Homeland Security

Richard Brackney
Department of Defense

Kevin Brady
Motorola, Incorporated

Roger Callahan
Information Assurance Advisory, LLC

Frank Caruso
Department of Defense

Agnes Chan
Northeastern University

Bei-Tseng Chu
University of North Carolina – Charlotte

Erin Comer
Booz Allen Hamilton

Kathryn Condello
Qwest Communications International, Incorporated

Guy Copeland
Computer Sciences Corporation

Michael Daly
Raytheon Company

Robert Dix
Juniper Networks, Incorporated

Dave Dobbs
Northrop Grumman Corporation

Kathy Downie
Advanced Research & Technology Center

John Edwards
Nortel Networks Corporation

Douglas Egan
Computer Sciences Corporation

David Ehinger
Rolls-Royce North America

Al Evans
Computer Sciences Corporation

Perry Fergus
Booz Allen Hamilton

Norman Fosmire
National Protection and Program Development Directorate, Department of Homeland Security

Mark Gannon
Motorola, Incorporated

Kiesha Gebreyes
National Communications System, Department of Homeland Security

Pradeep Goel
Science Applications International Corporation

Seymour Goodman
Georgia Tech

Sarah Greenwood
Booz Allen Hamilton

Gary Grube
Motorola, Incorporated

Douglas Hanson
Motorola, Incorporated

Elizabeth Hart
Booz Allen Hamilton

Charles Hearne
LGS Innovations, LLC

Ronda Henning
Harris Corporation

Mike Hickey
Verizon Communications, Incorporated

Lynn Hitchcock
Raytheon Company

Phillip Hodgins
Centre for the Protection of National Infrastructure

Anthony Jones
Raytheon Company

Kevin Kane
Harris Corporation

Richard Kane
Motorola, Incorporated

Frank Kapica
Mesirow Financial

Aggelos Katsaggelos
Northwestern University

Henry Kluepfel
Science Applications International Corporation

Maggie Lackey
Industry Canada

Marvin Langston
Science Applications International Corporation

Bob Leafloor
Industry Canada

Rosemary Leffler
AT&T, Incorporated

Mark Lohman
Computer Sciences Corporation

James Madon
National Communication Systems,
Department of Homeland Security

Maneck Master
Telcordia Technologies, Incorporated

James Mathis
Motorola, Incorporated

Peggy Matson
Motorola, Incorporated

Ernest McDuffie
National Coordination Office for Networking and Information Technology Research and Development

Tom Messerges
Motorola, Incorporated

Thomas Mihm
Motorola, Incorporated

Morris Moore
Motorola, Incorporated

Susan Moore
US Department of Agriculture

Timothy Moran
Science Applications International Corporation

Petros Mouchtaris
Telcordia Technologies, Incorporated

Trefor Munn-Venn
The Conference Board of Canada

Bruce Oberlies
Motorola, Incorporated

Thad Odderstol
National Communications System,
Department of Homeland Security

Clifton Poole
Raytheon Company

William Russ
Raytheon Company

Anthony Rutkowski
VeriSign, Incorporated

Ali Saidi
Motorola, Incorporated

Daniel Santos
US Nuclear Regulatory Commission

Siafa Sherman
Nortel Networks Corporation

Leslie Sibick
Department of Homeland Security

Julie Thomas
AT&T, Incorporated

Raymond Thorpe
Harris Corporation

Louise Tucker
Telcordia Technologies, Incorporated

Zach Tudor
SRI International

Chris Watson
Department of Homeland Security

Ed White
McAfee, Incorporated

Sterling Winn
Intelsat, Ltd.

Dawane Young
Booz Allen Hamilton

James Zok
Computer Sciences Corporation

Speakers' Remarks

Welcome/Introduction – Mr. Gary Grube

NSTAC RDX – Welcome

Making the Technology Connection

Gary Grube
Motorola Senior Fellow

Introductory thoughts to fuel later discussions on these topics:
Emergency Communications Response Networks
Convergent Technologies
Defending Cyberspace
Identity Management
Emerging Technologies

- World population : 4 births per second
- Mobile phones : 25 sold per second

Government & Public Safety

Significant Technology Shifts

1

Technology shift

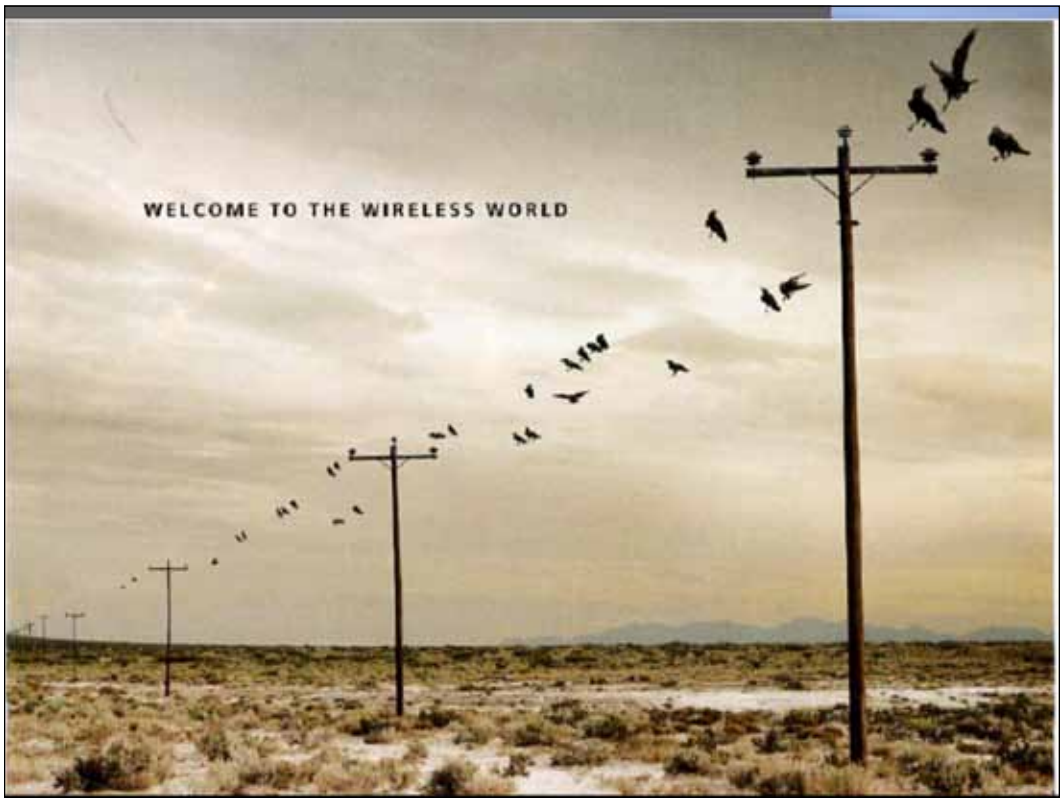
WWW

Implications

Business models flourish that can leverage massive peer-to-peer activity.

Digital content and information now becomes more valuable.

Government & Public Safety



Significant Technology Shifts

3

Technology shift

Cloud computing

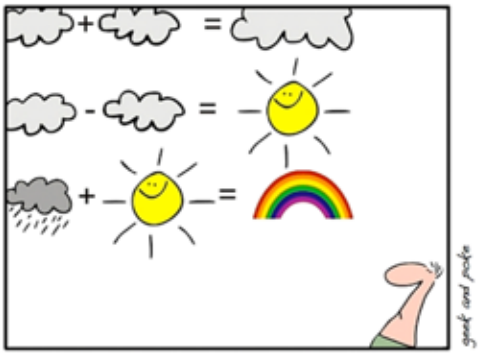
GARTNER Aug 2008: "Organisations are switching from company-owned hardware and software assets to per-use service-based models. This will impact the industry in various ways," Mr. Tully said. "The projected shift to cloud computing, for example, will result in dramatic growth in IT products in some areas and in significant reductions in other areas. In general, assets will be utilized with greater efficiency, and we are assuming that the overall effect on market growth will be neutral. We also recognize that there is considerable upside potential for higher growth."
"Software as a Service (SaaS)/cloud computing, service oriented architecture (SOA)/Web 2.0, and open source software are causing huge changes to the software market. Many of these factors are impacting market growth as enterprises replace assets with per-use services."

Government & Public Safety

Implications

Software as a Service (SaaS)

Non-stop computing and never-lose-it storage.



SIMPLY EXPLAINED – PART 17: CLOUD COMPUTING

Significant Technology Shifts

4

Technology shift

Multi-band/mode Devices

- SDR IC platforms
- Large color displays
- Morphing displays
- Haptic feedback

Intelligence at the edge

Implications

All-in-one device or specialty devices with a few tricks.

Coverage = aggregate of each network

Improved efficiency, fun, self actualization!

Knowledge Management
- Communication
- Search
- Data store/recall
- Analysis
- Presentation
- Decision Making

WHAT'S HOT: PERSONAL CONTEXT

Government & Public Safety

Significant Technology Shifts

5

Technology shift

Web based hosted applications

- Digital content
- Social networking

Implications

Context and more becomes important to find just what you need, to stay in touch without being smothered

Content eclipses access as a revenue generator

Aggregation more valuable

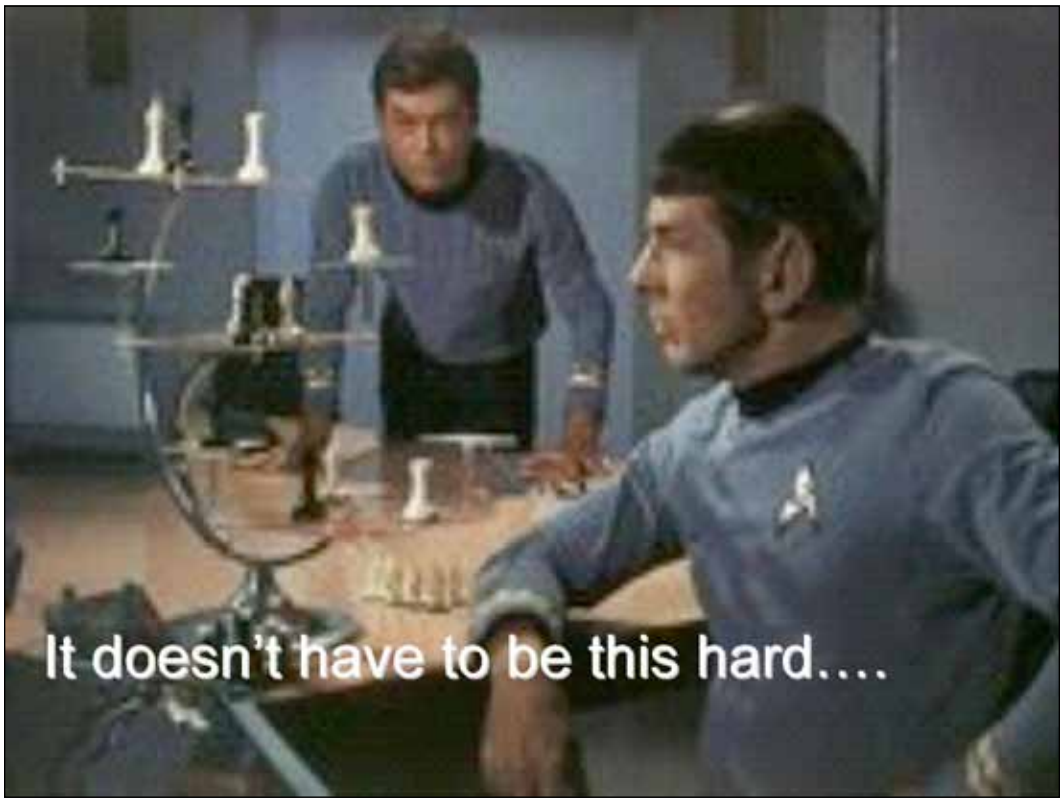
Google

YouTube Broadcast Yourself™

myspace.com a place for friends

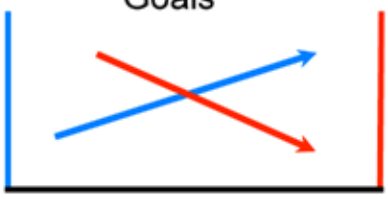
facebook

Government & Public Safety



the challenge

Value
- Function
- utility



Approaches to leveraging new technologies:
- Create new assets
- Extract continued value from current assets
- Enable improved process and policies

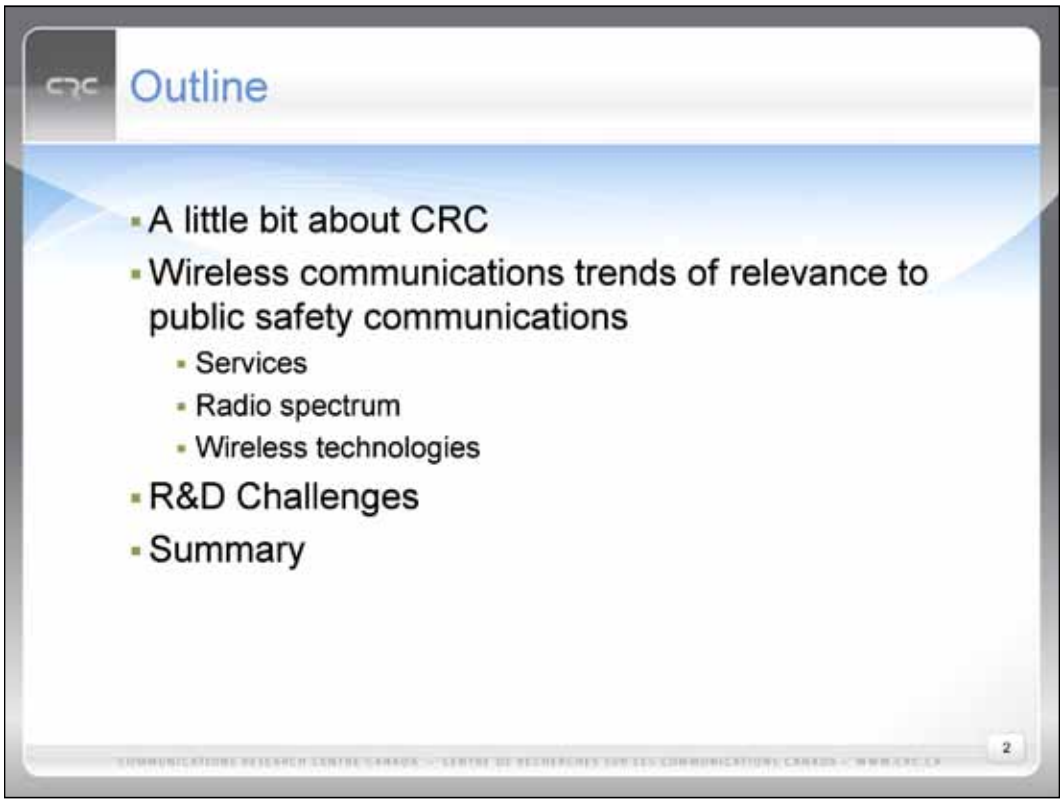
A challenge to us all:

"Innovate to Migrate"

Have a great workshop…

Government & Public Safety

Keynote Address – Dr. Veena Rawat



About Communications Research Centre

- Canadian federal government laboratory.
- Conducts R&D in communications technologies and systems. (wireless, satellite, broadcasting and fiber).
- Provides technical expertise to Industry Canada for the development of telecom standards, regulations and policy … and advice for S&T policies.
- Carries out R&D for other federal departments and agencies (e.g. National Defence, Canadian Space Agency, Public Safety Canada, Communications Security Establishment…).
- Partners with industry, universities, international research organizations; and technology transfer.
- 230 technical staff

3

About CRC

Strategic Priorities

- Radio Spectrum
- Broadband Access
- Defence Communications
- Network Security & Public Safety
- Internet and Convergence
- Applications

Core Competencies

- Wireless Systems
- Communications Networks
- Radio Fundamentals
- Interactive Multimedia
- Photonics (Optical Comms)

4

Public Safety and Emergency Response Communications

Current Situation

- Varied radio communications systems used by different public agencies (police, fire, health; municipal, state/provincial, federal)
- Use of dedicated and commercially-provided systems
- Interoperability challenges

Requirements

- Communications interoperability amongst PS/ER organizations
- Voice, data, images, video
- Increased bandwidth; radio spectrum
- Reliability
- Security

COMMUNICATIONS RESEARCH CENTRE CANADA ▪ CENTRE DE RECHERCHES SUR LES COMMUNICAT

Wireless Communications Trends……

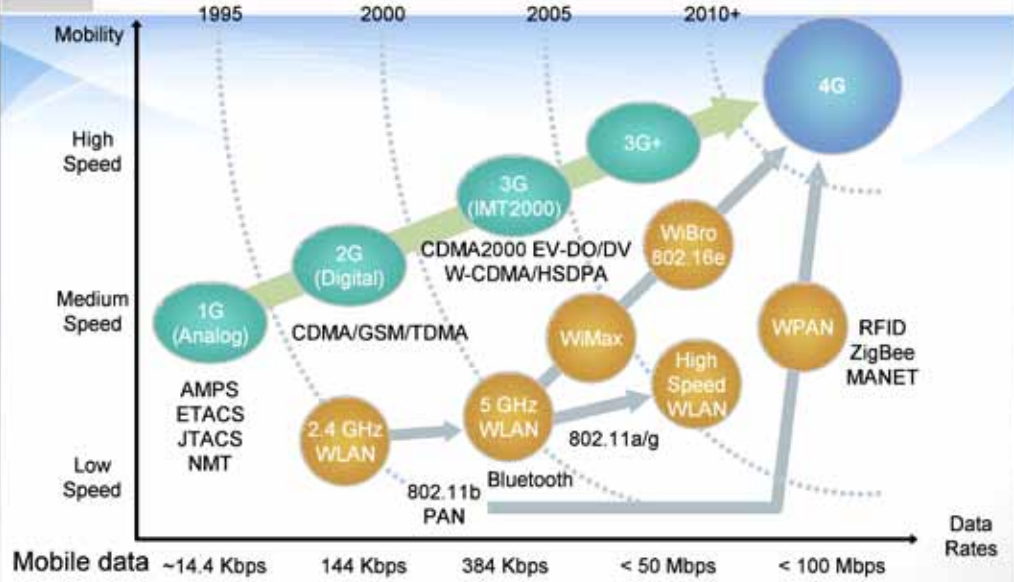
Potential to impact/ alter public safety communications

Communications Trends

Voice, internet services anywhere, anytime, any platform

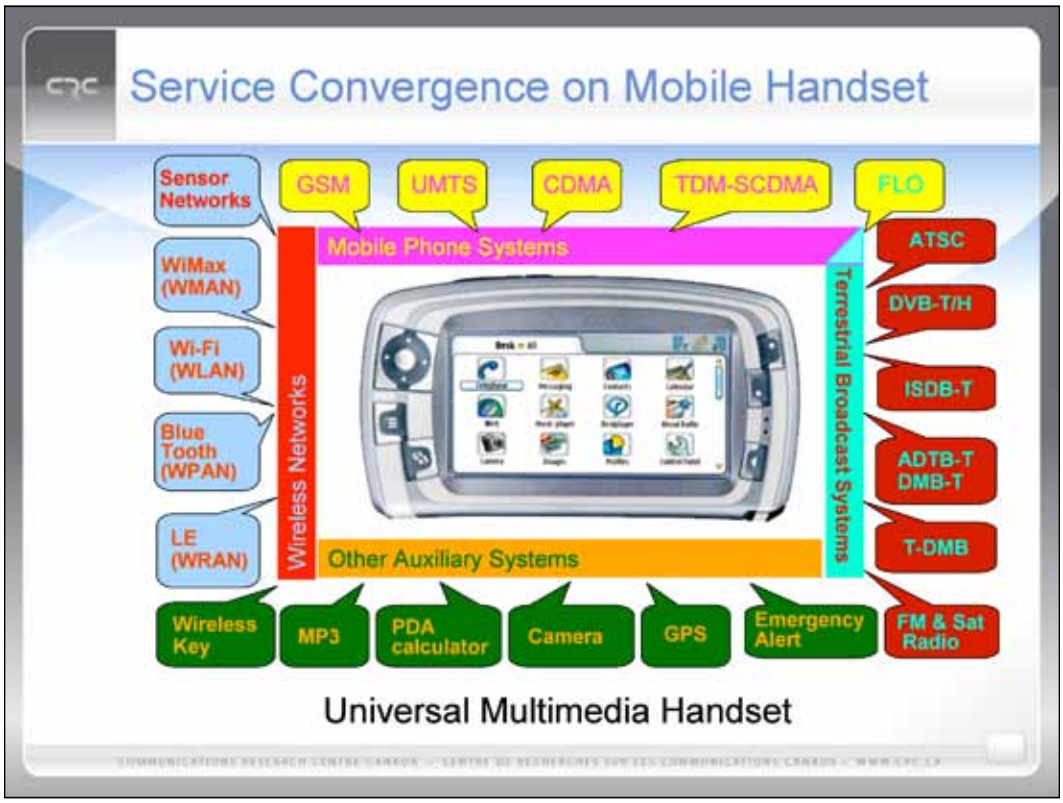
- Ubiquitous wireless – mobile, fixed wireless access
  - Cellular - 3G, 4G and beyond
  - Wireless internet access - Wi-Fi, Wi-Max
  - Personal area networks (Bluetooth..)
  - Satellite communications – mobile services, cellular backhaul, internet access extension (e.g. DVB-RCS)
- Convergence – Cellular and fixed wireless access
- Location-awareness (GPS) and location-aware services

Mobile Wireless Access Evolution



Source: 4G Roadmap & Emerging Communication Technologies, Artech House, 2005


Broadcasting Service Trends
Video/Television and radio anywhere, anytime, any platform
Traditional Radio and TV Broadcasting
Over-the-Air
Cable
Satellite
Emerging Delivery Technologies
Mobile TV (3G cellular, DVB-H, ATSC-H/M..)
Internet TV (streaming, client-server, P2P..)
IPTV (delivery of broadcast-quality video over broadband network - xDSL, fibre)
WiFI/WiMax
COMMUNICATIONS RESEARCH CENTRE CANADA ▪ CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA ▪ WWW.CRC.CA
9

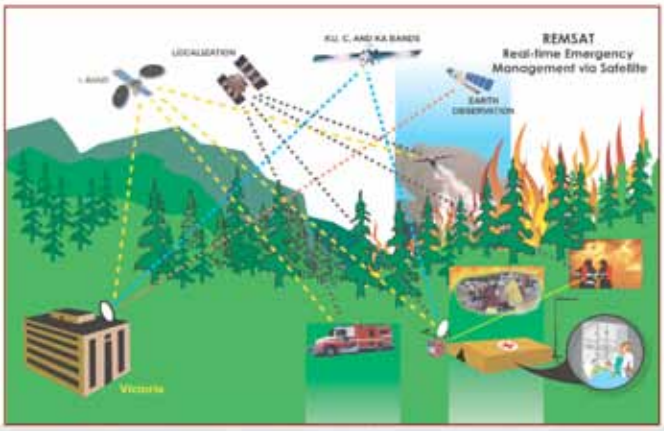

Service Convergence on Mobile Handset
Sensor Networks
GSM
UMTS
CDMA
TDM-SCDMA
FLO
WiMax (WMAN)
Wi-Fi (WLAN)
Blue Tooth (WPAN)
LE (WRAN)
Wireless Networks
Mobile Phone Systems
Terrestrial Broadcast Systems
ATSC
DVB-T/H
ISDB-T
ADTB-T DMB-T
T-DMB
Other Auxiliary Systems
Wireless Key
MP3
PDA calculator
Camera
GPS
Emergency Alert
FM & Sat Radio
Universal Multimedia Handset

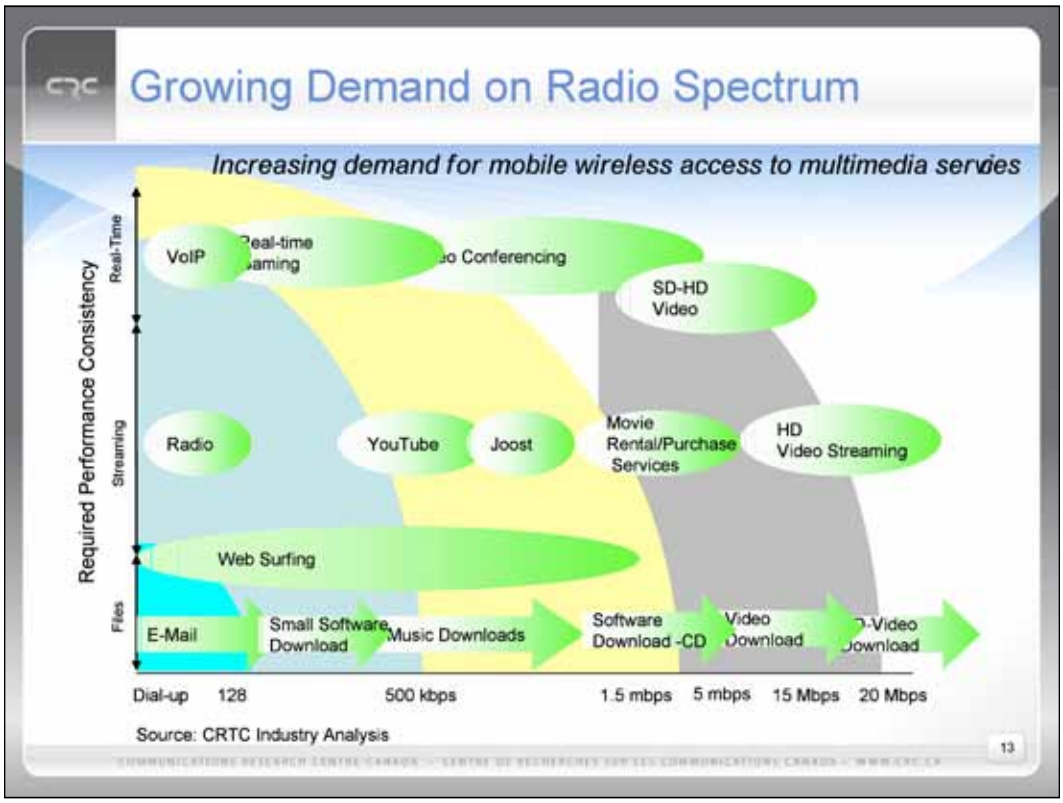
Emergency Alerting Over Wireless Networks

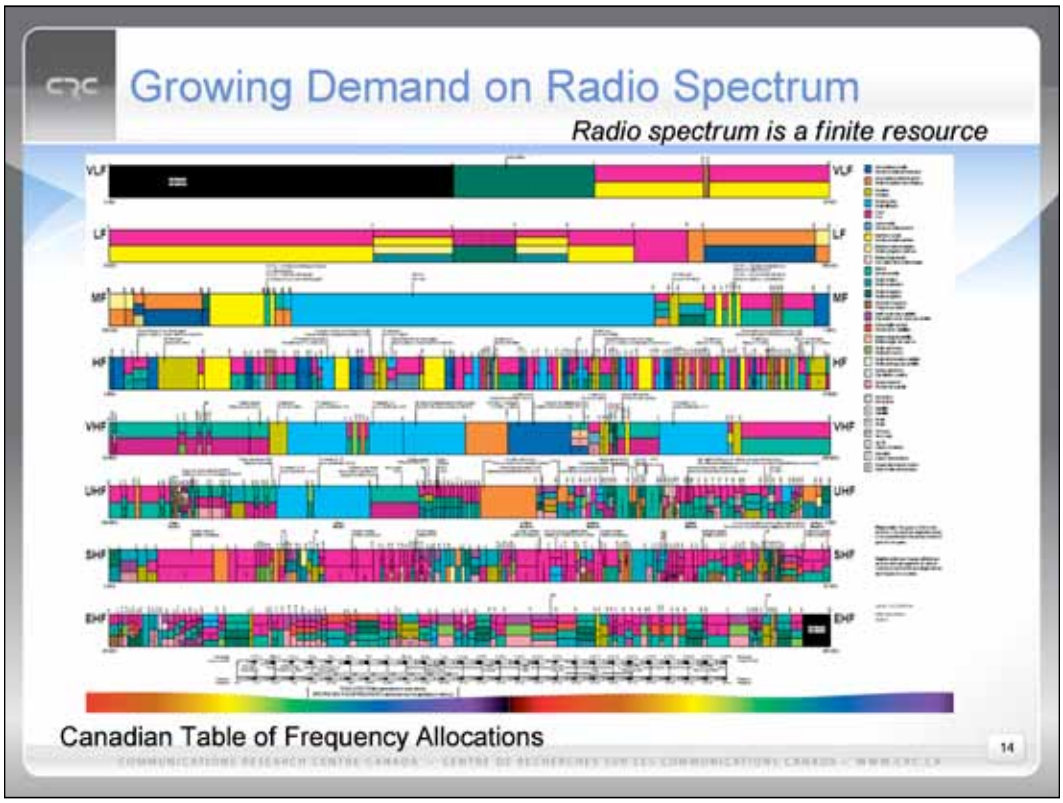
- *Traditional* - Radio and TV broadcasting
- *Emerging* - Alerting to handheld wireless devices
  - Cellular – SMS
    - Challenges include – timely delivery of message to all; network congestion; network failure
  - New multimedia digital broadcasting systems
    - Broadcast networks are efficient means to deliver information to a large number of users
    - Satellite and terrestrial delivery
    - DMB, IBOC, ATSC-H/M, DVB-H…

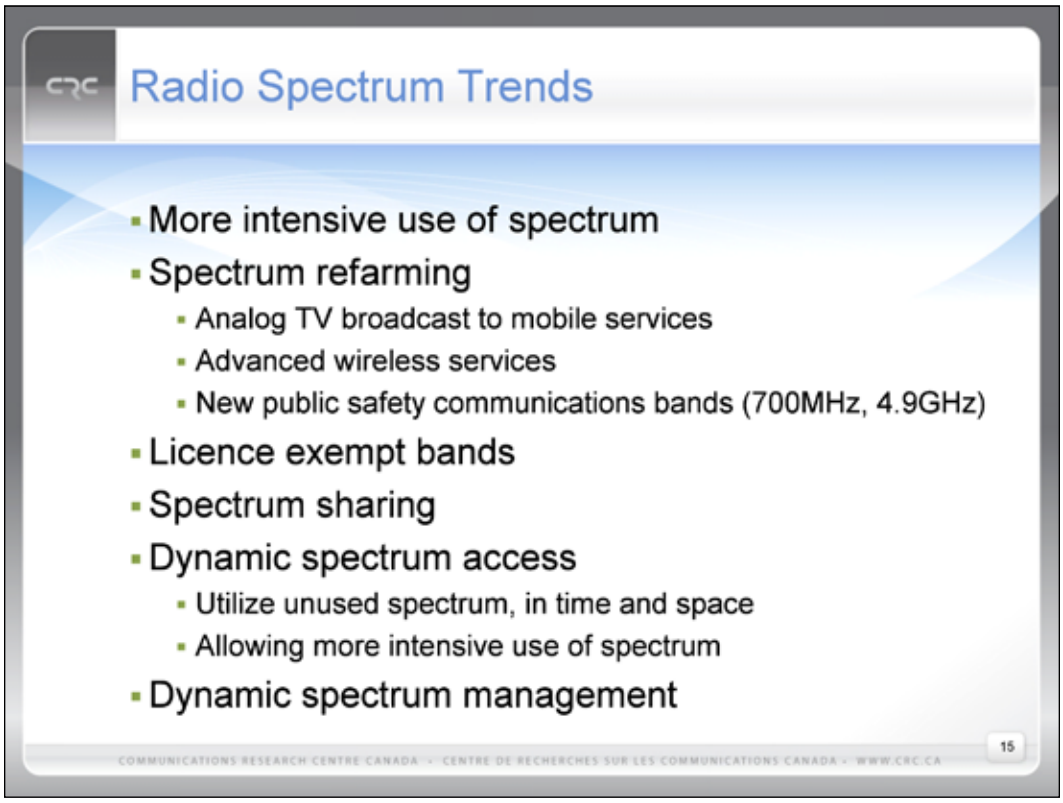
Other Satellite Communications Applications

- Search and rescue satellite (SARSAT, MEOSAR..)
- Emergency management via satellite




Growing Demand on Radio Spectrum
Increasing demand for mobile wireless access to multimedia services
Required Performance Consistency
Real-Time
Streaming
Files
VoIP
Real-time Gaming
Video Conferencing
SD-HD Video
Radio
YouTube
Joost
Movie Rental/Purchase Services
HD Video Streaming
Web Surfing
E-Mail
Small Software Download
Music Downloads
Software Download -CD
Video Download
Video Download
Dial-up
128
500 kbps
1.5 mbps
5 mbps
15 Mbps
20 Mbps
Source: CRTC Industry Analysis
13


Growing Demand on Radio Spectrum
Radio spectrum is a finite resource
VLF
LF
MF
HF
VHF
UHF
SHF
EHF
Canadian Table of Frequency Allocations
14


Radio Spectrum Trends
More intensive use of spectrum
Spectrum refarming
Analog TV broadcast to mobile services
Advanced wireless services
New public safety communications bands (700MHz, 4.9GHz)
Licence exempt bands
Spectrum sharing
Dynamic spectrum access
Utilize unused spectrum, in time and space
Allowing more intensive use of spectrum
Dynamic spectrum management
15


Wireless Technology Trends……
Potential to impact/ alter public safety communications
16

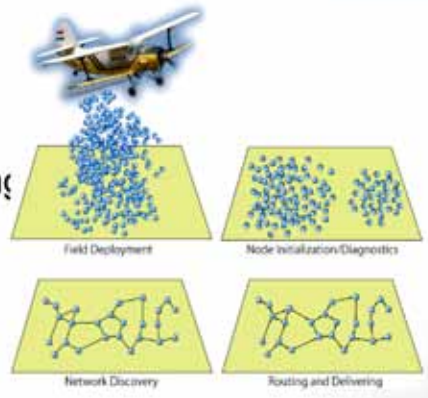
Key Technology Enablers

- Advances in digital signal processing technology
- Advances in A/D, D/A converters
- Increasing computing power
- Open software
- Software defined radio
- Cognitive radio

17

Wireless Sensor Networks

- Wireless network of distributed autonomous sensors to monitor physical and environmental conditions
- Applications – security, monitoring, detection, tracking
  - Border
  - Hazardous zones



18

Software Defined Radio - SDR

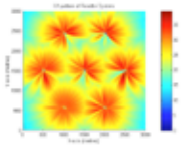
- Radio in which some or all of the physical layer functions are software defined
- SDRs could simultaneously support multiple protocols across a range of spectrum
- SDR Benefits
  - Interoperability
  - Reconfigurability

19

COMMUNICATIONS RESEARCH CENTRE CANADA • CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA • WWW.CRC.CA

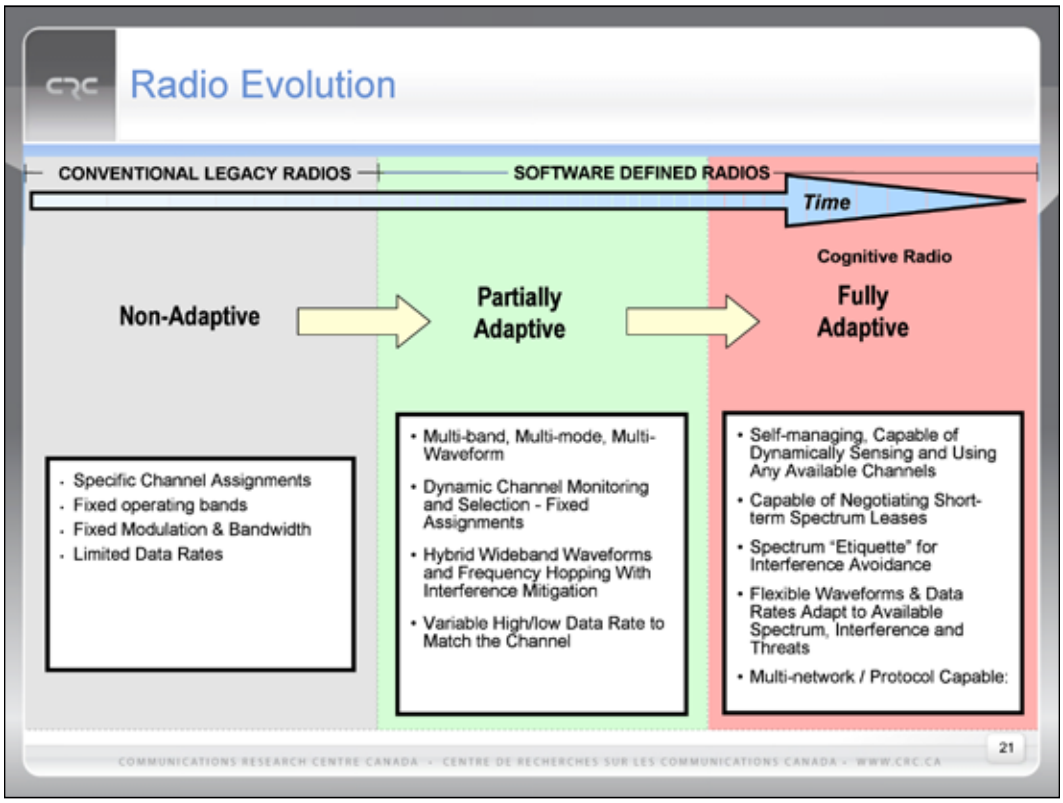
Cognitive Radio

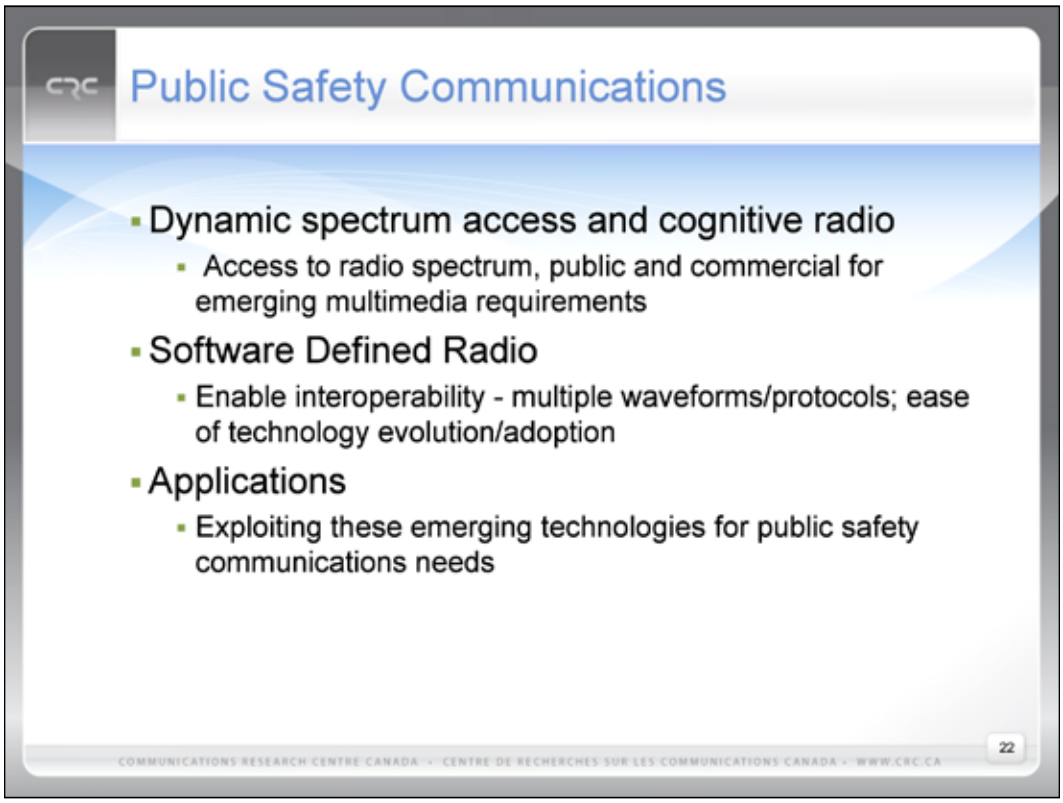
- A radio that senses and is aware of its operational environment and can dynamically and autonomously adjust its radio operating parameters accordingly
- Enables spectrum agile radios and dynamic spectrum access
- Enables improved spectral efficiency, through adaptive optimized use of waveforms, modulation, network access

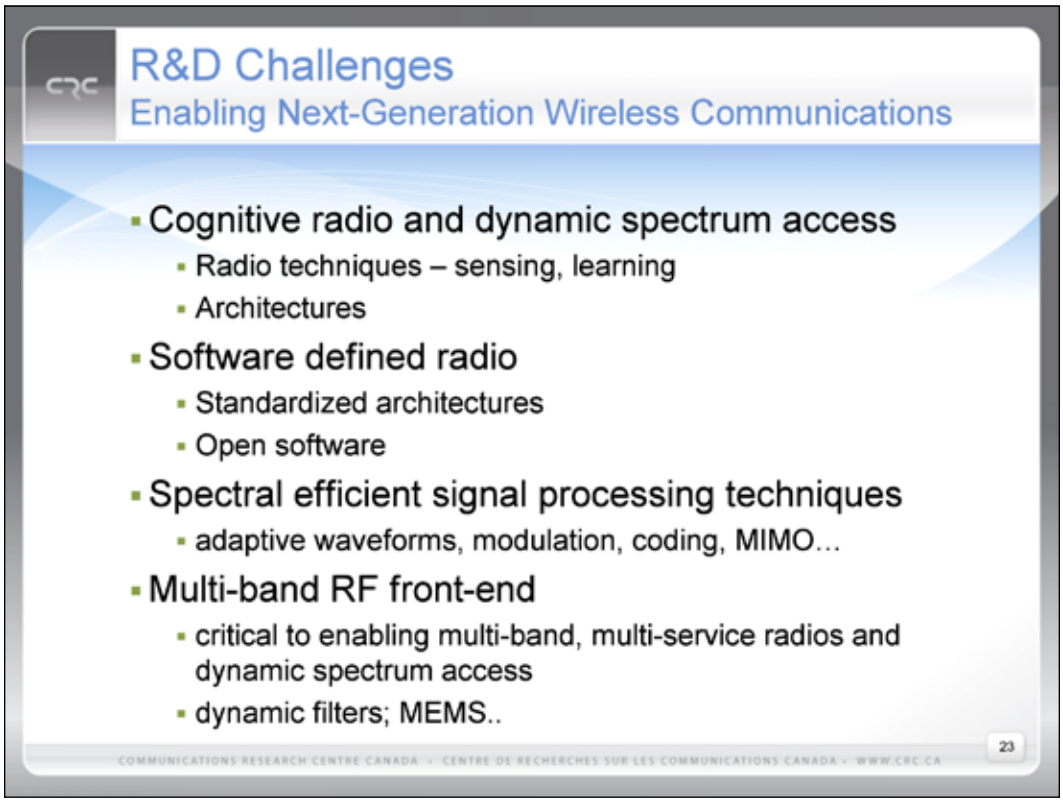


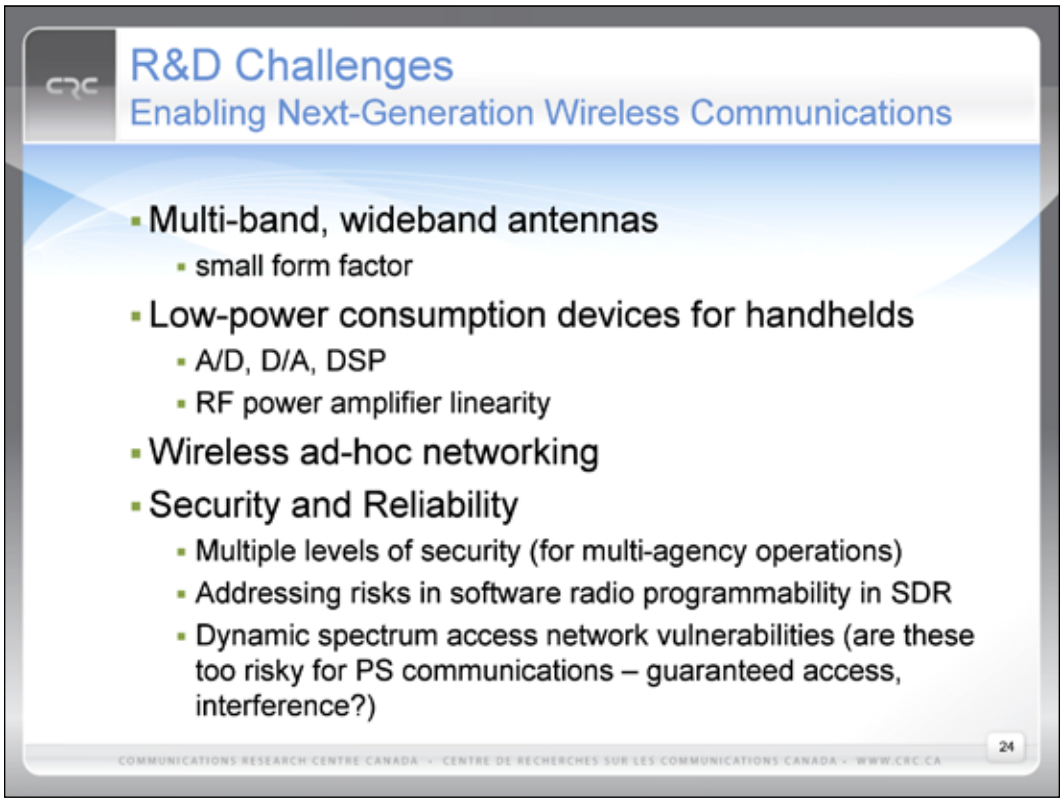
20

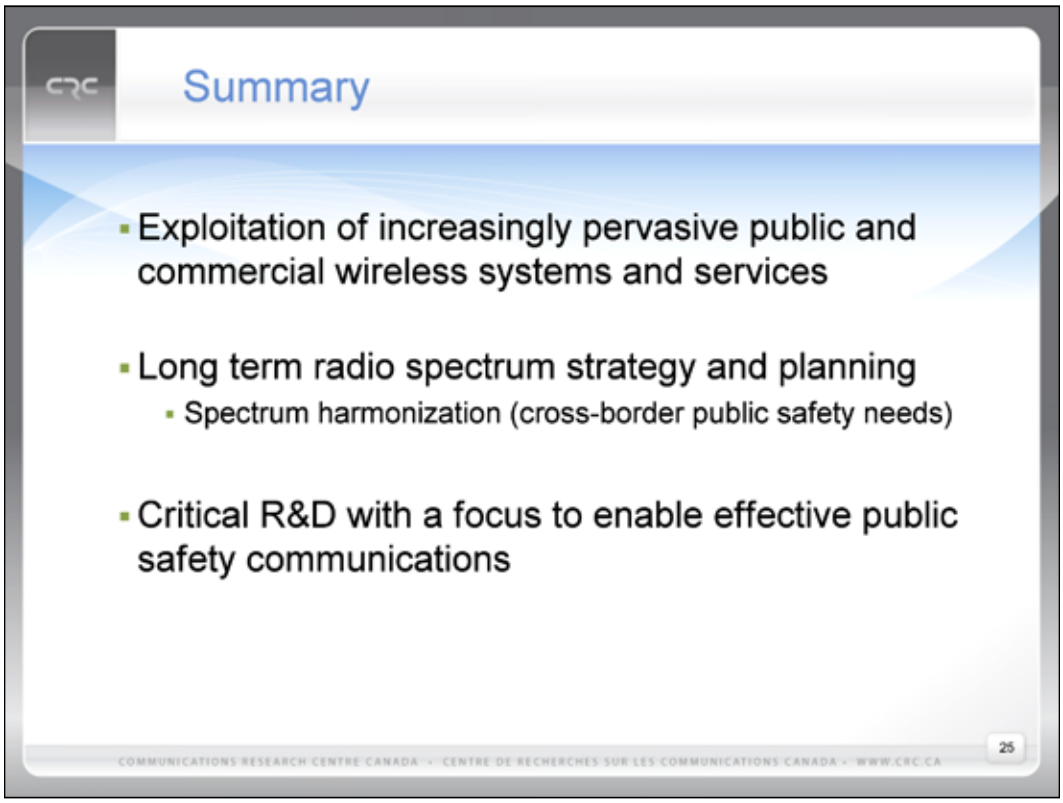
COMMUNICATIONS RESEARCH CENTRE CANADA • CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA • WWW.CRC.CA


Radio Evolution
CONVENTIONAL LEGACY RADIOS
SOFTWARE DEFINED RADIOS
Time
Cognitive Radio
Non-Adaptive
Partially Adaptive
Fully Adaptive
Specific Channel Assignments
Fixed operating bands
Fixed Modulation & Bandwidth
Limited Data Rates
Multi-band, Multi-mode, Multi-Waveform
Dynamic Channel Monitoring and Selection - Fixed Assignments
Hybrid Wideband Waveforms and Frequency Hopping With Interference Mitigation
Variable High/low Data Rate to Match the Channel
Self-managing, Capable of Dynamically Sensing and Using Any Available Channels
Capable of Negotiating Short-term Spectrum Leases
Spectrum "Etiquette" for Interference Avoidance
Flexible Waveforms & Data Rates Adapt to Available Spectrum, Interference and Threats
Multi-network / Protocol Capable:
21
COMMUNICATIONS RESEARCH CENTRE CANADA • CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA • WWW.CRC.CA

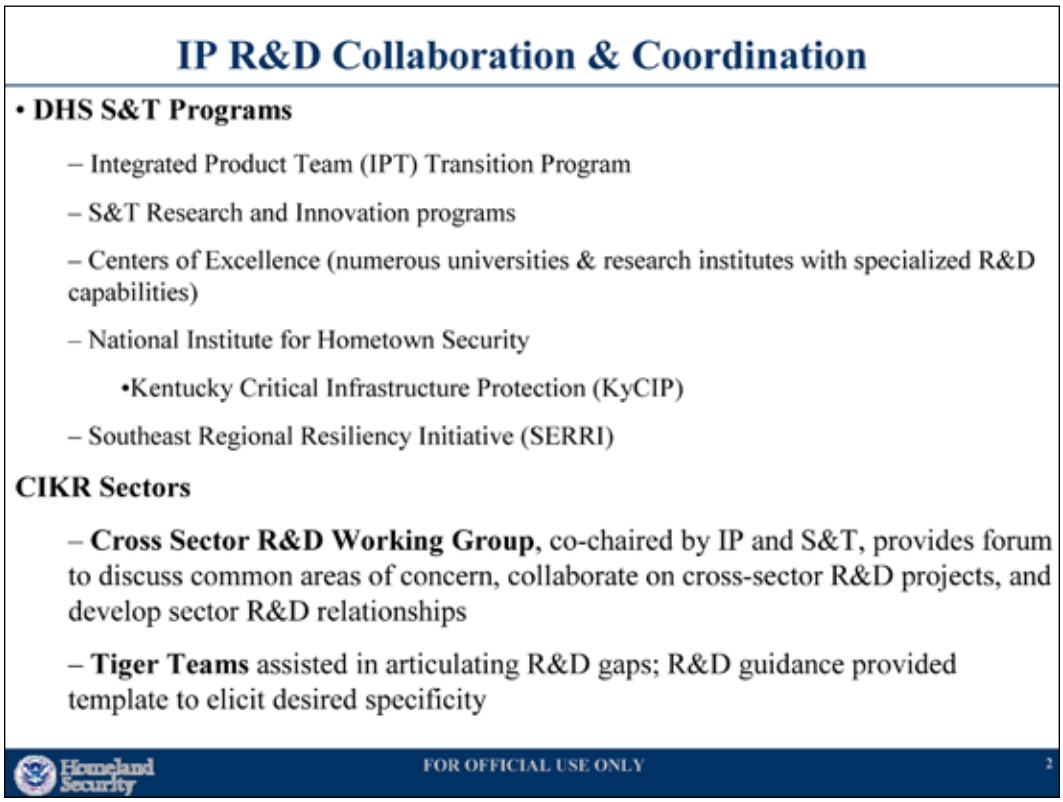

Public Safety Communications
Dynamic spectrum access and cognitive radio
Access to radio spectrum, public and commercial for emerging multimedia requirements
Software Defined Radio
Enable interoperability - multiple waveforms/protocols; ease of technology evolution/adoption
Applications
Exploiting these emerging technologies for public safety communications needs
22
COMMUNICATIONS RESEARCH CENTRE CANADA • CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA • WWW.CRC.CA


R&D Challenges
Enabling Next-Generation Wireless Communications
Cognitive radio and dynamic spectrum access
Radio techniques – sensing, learning
Architectures
Software defined radio
Standardized architectures
Open software
Spectral efficient signal processing techniques
adaptive waveforms, modulation, coding, MIMO…
Multi-band RF front-end
critical to enabling multi-band, multi-service radios and dynamic spectrum access
dynamic filters; MEMS..
23


R&D Challenges
Enabling Next-Generation Wireless Communications
Multi-band, wideband antennas
small form factor
Low-power consumption devices for handhelds
A/D, D/A, DSP
RF power amplifier linearity
Wireless ad-hoc networking
Security and Reliability
Multiple levels of security (for multi-agency operations)
Addressing risks in software radio programmability in SDR
Dynamic spectrum access network vulnerabilities (are these too risky for PS communications – guaranteed access, interference?)
24


Summary
Exploitation of increasingly pervasive public and commercial wireless systems and services
Long term radio spectrum strategy and planning
Spectrum harmonization (cross-border public safety needs)
Critical R&D with a focus to enable effective public safety communications
25
COMMUNICATIONS RESEARCH CENTRE CANADA • CENTRE DE RECHERCHES SUR LES COMMUNICATIONS CANADA • WWW.CRC.CA

Presentation – Ms. Leslie Sibick



NIPP R&D Requirements Process

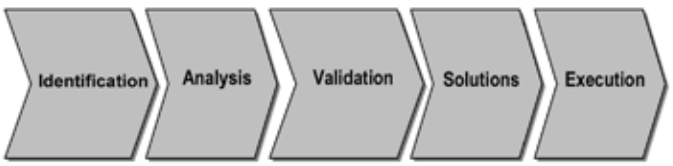
- Vision – A transparent, repeatable and honest R&D requirements program to mitigate long-term National Homeland Security risks
- Mission – Assist NIPP stakeholders in identification and articulation of strategic R&D requirements, then facilitate coordination with S&T and others to address those capability gaps as effectively and efficiently as possible
- Goal – Actively identify and align sector needs with expertise in academia, research and analysis centers, S&T Centers of Excellence, research consortia, as well as IP-directed programs such as the National Infrastructure Simulation and Analysis Center (NISAC)

Homeland Security FOR OFFICIAL USE ONLY 3

Phases of NIPP R&D Requirements Process

Five phases to the NIPP R&D Requirements Process

- Identification: Sector R&D Requirements Identification
- Analysis: IP Collection & Analysis
- Validation: NIPP Requirements Steering Group Prioritization and Validation
- Solution Identification: Integrated Product Team (IPT) Process primarily
- Execution: R&D Project Execution and Implementation



Homeland Security FOR OFFICIAL USE ONLY 4

2008 Sector Annual Report Statistics

Public Health and Healthcare…23	Banking/Finance…3
Transportation..19	Energy…2
Water…15	Nuclear…2
Dams…13	Chemical…1
Agriculture/Food…12	Telecommunications…1
Information Technology…9	Postal/Shipping…0
Commercial Facilities…7	National Monuments and Icons…0
Government Facilities…7	Defense Industrial Base…0
Emergency Services…5	Critical Manufacturing…0

119 CIKR Sector Capability Gaps Received for 2008

Homeland Security FOR OFFICIAL USE ONLY 5

IP Risk-Informed R&D Prioritization Methodology

- **GOAL:** To compare all gaps against CIP R&D themes, SHIRA, and other criteria
  - IP/R&D Analysis Branch collects, organizes and catalogues the R&D requirements submitted by the 18 CIKR Sectors
  - IP/R&D Analysis Branch prepares prioritized list of requirements and develops set of basic recommendations to inform R&D related CIKR protection activities
  - Gaps analyzed against 1) classified terrorism risk documents, 2) all hazards risks, 3) Sector or division internal prioritization
  - Look for cross-sector/multi-sector issues
  - Look for DHS HQ issues that transcend sectors
- **OUTCOME:** Organized, cross-referenced, prioritized annual R&D requirements list with prioritization

Homeland Security FOR OFFICIAL USE ONLY 6


U.S. DEPARTMENT OF HOMELAND SECURITY
Homeland Security

Presentation – Dr. Doug Maughan

Dept. of Homeland Security Science & Technology Directorate

Current DHS Cyber Security RDTE&T Initiatives

NSTAC RDX
Schaumburg, IL
Sept 25-26, 2008

Douglas Maughan, Ph.D.
Program Manager, CCI
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170

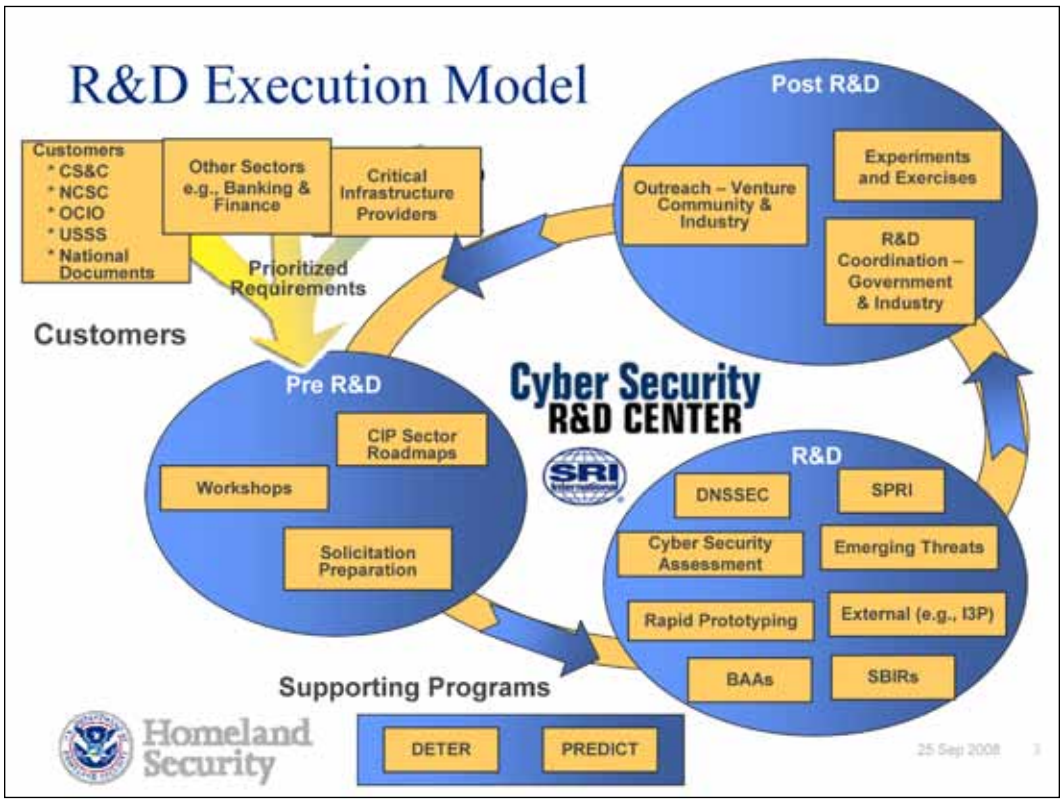
Homeland Security

Science and Technology (S&T) Mission

Conduct, stimulate, and enable **research, development, test, evaluation and timely transition** of homeland security capabilities to federal, state and local operational end-users.

Homeland Security

25 Sep 2008 2



Cyber Security Program Areas

- Information Infrastructure Security
  - Domain Name System Security (DNSSEC)
  - Secure Protocols for the Routing Infrastructure (SPRI)
  - Finance Sector Risk Mgmt Toolkit (Web*DECIDE)
- Cyber Security Research Tools and Techniques
  - Cyber Security Testbed (DETER)
  - Large Scale Datasets (PREDICT)
  - Experiments and Exercises
- Next Generation Technologies
  - BAA 04-17, BAA 07-09
- Other Activities (SBIR, RTAP, Emerging Threats, Outreach)

Homeland Security

25 Sep 2008 4

National Strategy to Secure Cyberspace

- The National Strategy to Secure Cyberspace (2003) recognized the DNS as a critical weakness
  - NSSC called for the Department of Homeland Security to coordinate public-private partnerships to encourage the adoption of improved security protocols, such as DNS
  - **The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS**. The Nation has a vital interest in ensuring that this work proceeds. **The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.**

Homeland Security

25 Sep 2008 5

DNSSEC Initiative Activities

- Roadmap published in February 2005; **Revised March 2007**
  - http://www.dnssec-deployment.org/roadmap.php
- DNSSEC testbed developed by NIST
  - http://www-x.antd.nist.gov/dnssec/
- Involvement with numerous deployment pilots
- Formal publicity and awareness plan including newsletter
  - http://www.dnssec-deployment.org/news/dnssecthismonth
- Working with Microsoft, Mozilla, OpenDNS and others to promote DNSSEC awareness in their software or projects

Homeland Security

25 Sep 2008 6

OMB memo on DNSSEC

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf

August 22, 2008

M-08-23

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Securing the Federal Government's Domain Name System Infrastructure
(Submission of Draft Agency Plans Due by September 5, 2008)

The efficient and effective use of our networks is important to promote a more citizen centered and results oriented government. The Government's reliance on the Internet to disseminate and provide access to information has increased significantly over the years, as have the risks associated with potential unauthorized use, compromise, and loss of the .gov domain space.

Almost every instance of network communication begins with a request to the Domain Name System (DNS) to resolve a human readable name for a network resource (e.g., www.usa.gov) into the technical information (e.g., Internet Protocol address) necessary to actually access the remote resource. This memorandum describes existing and new policies for deploying Domain Name System Security (DNSSEC) to all Federal information systems by December 2009

Secure Protocols for the Routing Infrastructure (SPRI)

- Border Gateway Protocol (BGP)
  - routing protocol that connects ISPs and subscriber networks together to form the Internet
  - used to exchange network *reachability inf ormation*
  - 1989: RFC 1105 – June 1989
    - Created based on Internet transition to Autonomous Systems
  - Final version: BGP-4 (RFC 1771-1774 – 3/95)
- Securing BGP
  - Secure BGP (BBN): 1998-2003
  - Secure Origin BGP (Cisco): 2000-2004
  - Many others ……

Homeland Security

25 Sep 2008 8

Elements of Secure BGP Failure

- Adding security to infrastructure protocols is VERY difficult
- Customer: Who is the actual "end customer" – ISPs or routing vendors or network engineers??
  - ISPs don't ask for secure products until end consumers complain about security issues
  - Routing vendors don't add security into their products until ISPs request those capabilities
  - Network engineers don't have a loud enough voice
- Bottom Line: Who's responsible for getting security into the global infrastructure?
- Will recent DEFCON attack demonstrations have any impact on the "key BGP players"?

Homeland Security

25 Sep 2008 9

SPRI Going Forward

- Working with ARIN to clean up existing database and legacy address space problem
  - Pre-1997 IP Addresses are not accounted for
- Working with ARIN and APNIC to deploy PKI between ICANN/IANA and registry and between registry and ISPs/customers
  - Pilot project with the American Registry for Internet Numbers (ARIN) and Asia-Pacific Network Information Center (APNIC) to add public key infrastructure to registration operations
- What else are we planning to do?
  - DHS S&T will be holding several routing security R&D workshops over the course of the next 12-18 months with the relevant parties
  - If you (or your company) are interested in participating, let me know

Homeland Security

25 Sep 2008 10

DHS / NSF Cyber Security Testbed

- **"Justification and Requirements for a National DDOS Defense Technology Evaluation Facility", July 2002**
- We still lack large-scale deployment of security technology sufficient to protect our vital infrastructures
  - Recent investment in research on cyber security technologies by government agencies (NSF, DARPA, armed services) and industry.
- One important reason is the lack of an experimental infrastructure and rigorous scientific methodologies for developing and testing next-generation defensive cyber security technology
- The goal is to create, operate, and support a researcher-and-vendor-neutral experimental infrastructure that is open to a wide community of users and produce scientifically rigorous testing frameworks and methodologies to support the development and demonstration of next-generation cyber defense technologies

Homeland Security

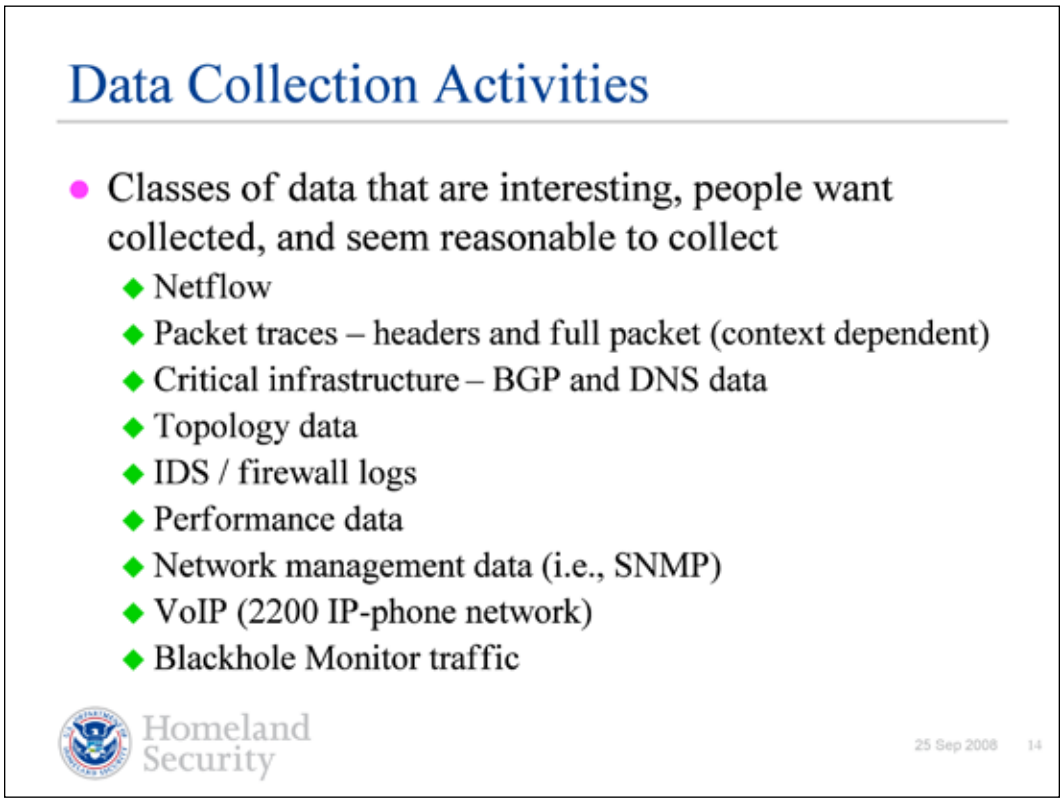
25 Sep 2008 11

DETER Users Map – over 70 sites

Homeland Security

25 Sep 2008 12


A Protected REpository for Defense of Infrastructure against Cyber Threats
PREDICT Program Objective
"To advance the state of the research and commercial development (of network security 'products') we need to produce datasets for information security testing and evaluation of maturing networking technologies."
Rationale / Background / Historical:
Researchers with insufficient access to data unable to adequately test their research prototypes
Government technology decision-makers with no data to evaluate competing "products"
End Goal: Improve the quality of defensive cyber security technologies
Homeland Security
25 Sep 2008
13


Data Collection Activities
Classes of data that are interesting, people want collected, and seem reasonable to collect
Netflow
Packet traces – headers and full packet (context dependent)
Critical infrastructure – BGP and DNS data
Topology data
IDS / firewall logs
Performance data
Network management data (i.e., SNMP)
VoIP (2200 IP-phone network)
Blackhole Monitor traffic
Homeland Security
25 Sep 2008
14

PREDICT Information

- https://www.predict.org

- DHS Privacy Impact Assessment
  - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_predict.pdf

Homeland Security

25 Sep 2008 15

Cyber Security R&D Broad Agency Announcement (BAA)

- A critical area of focus for DHS is the development and deployment of technologies to protect the nation's cyber infrastructure including the Internet and other critical infrastructures that depend on computer systems for their mission. The goals of the Cyber Security Research and Development (CSRD) program are:
  - To perform research and development (R&D) aimed at **improving the security of existing deployed technologies** and to ensure the security of new emerging systems;
  - To **develop new and enhanced technologies** for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure.
  - To **facilitate the transfer of these technologies** into the national infrastructure as a matter of urgency.
- **http://www.hsarpabaa.com**

Homeland Security

25 Sep 2008 16

BAA Program / Proposal Structure

- **NOTE: Deployment Phase = Test, Evaluation, and Pilot deployment in (DHS) "customer" environments**
- Type I (New Technologies)
  - New technologies with an applied research phase, a development phase, and a deployment phase (optional)
    - Funding not to exceed 36 months (including deployment phase)
- Type II (Prototype Technologies)
  - More mature prototype technologies with a development phase and a deployment phase (optional)
    - Funding not to exceed 24 months (including deployment phase)
- Type III (Mature Technologies)
  - Mature technology with a deployment phase only.
    - Funding not to exceed 12 months

Homeland Security

25 Sep 2008 17

BAA 04-17 Technical Topic Areas

- System Security Engineering
  - Vulnerability Prevention
  - Vulnerability Discovery and Remediation
  - Cyber Security Assessment (i.e., Metrics)
- Security of Operational Systems
  - Security and Trustworthiness for Critical Infrastructure Protection
  - Wireless Security
- Investigative and Prevention Technologies
  - Network Attack Forensics (e.g., Traceback)
  - Technologies to Defend against Identity Theft

Homeland Security

25 Sep 2008 18

BAA04-17 Awards

TTA	Type	ID	PI Organization	Full Proposal Title	Funding Amt.
1	II	3	University of California, Irvine	Adding Mandatory Access Control to Java VMs	$312,483
2	I	5	GrammaTech, Inc	Model Checking Software Binaries	$442,011
2	I	9	Stanford University	Open Source Hardening Project	$1,241,276
2	II	1	Komoku, Inc.	Copilot - A High Assurance and Independent Security Auditor	$1,165,416
2	II	3	Georgia Institute of Technology	Preventing SQL Code Injection by Combining Static and Runtime Analysis	$390,019
3	II	5	University of Delaware	Benchmarks for evaluation of DDoS defense systems	$533,716
4	I	1	Princeton University	Incrementally Deployable Security for Interdomain Routing	$312,483
4	II	13	Adventium Labs	Embedded Firewall for Robust Protection of Mission Critical Operations	$821,796
4	II	20	George Mason University	Enhanced Topological Vulnerability Analysis and Visualization	$1,100,000
4	III	2	Telcordia Technologies	AVACC: Automated Vulnerability Assessment of Critical Cyber-Infrastructure Through Policy-based Configuration Synthesis	$500,000
5	I	4	University of Michigan, Ann Arbor	Secure Coordination and Communication in a Crisis Using Hand-held Devices	$1,352,549
5	I	8	Dartmouth College	M.A.P. (Measure, Analyze, Protect): security through measurement for wireless LANs	$1,698,545
6	I	1	BBN Technologies	ZombieStones: Attack Tracing Across Events Separated in Time	$384,892
6	II	4	Southwest Research Institute	Single Packet IP Traceback Through Internet Autonomous Systems	$1,224,799
7	I	2	Stanford University	SpoofGuard Anti-Phishing Technologies	$766,671
7	II	4	SPARTA, Inc.	Phisherman	$887,142
7	II	7	BBN	PhishBouncer- An Architectural Approach to Defending Against Phishing Attacks	$749,639

Homeland Security

- 9 Academic (CA,GA,DE,NJ,VA,MI,NH)
- 8 Private Sector (NY,MD,MN,NJ,MA,TX)

25 Sep 2008 19

BAA 04-17 Accomplishments

- Komoku, Inc.
  - Rootkit detection and mitigation technology
    - Company purchased by Microsoft in March 2008
- George Mason University / Symantec
  - Network topology vulnerability analysis
    - Deployed at several government agencies (FAA, AFRL)
- Telcordia
  - Automated Vulnerability Assessment Tool
    - Deployed at SEC; Under consideration for S&T CIO pilot
- Stanford University
  - Anti-phishing technologies
    - Technology transferred to RSA, Microsoft, Mozilla, Google

Homeland Security

25 Sep 2008 20

BAA 07-09 Technical Topic Areas

- Botnets and Other Malware: Detection and Mitigation
- Composable and Scalable Secure Systems
- Cyber Security Metrics
- Network Data Visualization for Information Assurance
- Internet Tomography / Topography
- Routing Security Management Tool
- Process Control System Security
  - Secure and Reliable Wireless Communication for Control Systems
  - Real-Time Security Event Assessment and Mitigation
- Data Anonymization Tools and Techniques
- Insider Threat Detection and Mitigation

Homeland Security

25 Sep 2008 21

BAA07-09 Awards

TTA	Type	PI Organization	Paper Title	Time	Proposed Funding
1	II	Georgia Institute of Technology	Countering Botnets: Anomaly-Based Detection, Comprehensive Analysis, and Efficient Mitigation	24	$ 1,050,730
2	I	IBM Thomas J. Watson Research Center	Montage: A Methodology for Designing Composable End-To-End Secure Distributed Systems	36	$ 900,000
2	II	Secure64 Software Corporation	Automating the Chain of Trust: Secure Interzone Key Management for Large Scale DNSSEC Deployments (Project Acronym: SCOTTY)	36	$ 1,242,815
2	II	Packet Clearing House, Inc.	INOC-DBA, VoIP Network Security	24	$ 600,000
4	I	CA	FloVIS: Flow Visualization System	30 + 6	$ 925,050
4	II	Secure Decisions division of Applied Visions, Inc.	Visualization Toolkit for NetFlow Analytics	12 + 10	$ 617,098
5	I	The Regents of the University of California; UC San Diego	leveraging the science and technology of Internet mapping for homeland security	18+12+6	$ 1,582,467
6	II	Colorado State University	WIT: A Watchdog System for Internet Routing	24	$ 1,500,000
6	III	Packet Clearing House, Inc.	BGP Routing Integrity Checker and Prefix-List Filter Generation Tool	12	$ 450,000
7	I	Digital Bond, Inc.	Passive Security Log Generation for Control Systems	12	$ 475,000
7	III	Sandia National Laboratories	Secure and Reliable Wireless Networks for Critical Infrastructure Facilities	12	$ 643,000
8	II	John Hopkins University	New Frameworks for Detecting and Minimizing Information Leakage in Anonymized Network Data	24	$ 928,682
9	I	Washington State University	Insider Threat Detection Using a Graph-based Approach	20 + 4	$ 327,667
9	II	Dolphin Technology Inc.	Document-based Management, Access Control and Security (DocuMACS)	18 + 6	$ 1,165,000
			TOTAL		$ 12,407,509

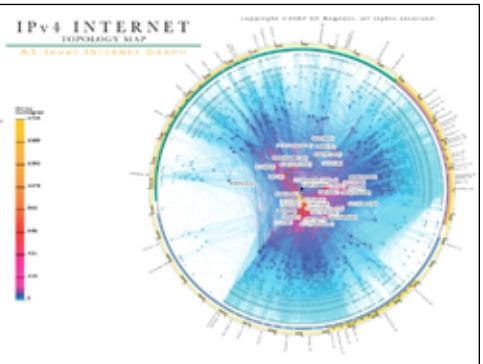
Homeland Security

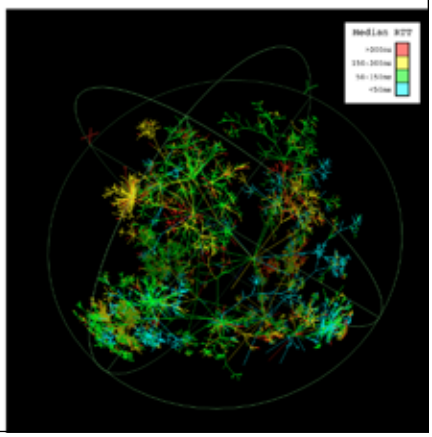
- 5 Academic (CA,GA,WA,CO,MD)
- 8 Private Sector (NY,CO,CA,FL)
- 1 National Lab (NM)

25 Sep 2008 22

Internet Mapping

- We don't know enough about the Internet, e.g, what keeps the system stable or drives it to instability.
- Improve critical national capabilities:
  - Situational awareness for homeland security purposes
  - Topology mapping
  - Internet measurement and analysis
- Address network science crisis
  - Scalability in system management, monitor deployment, measurement efficiency, resource utilization





Homeland Security

Routing Security Management

Pakistan Cuts Access to YouTube Worldwide

The New York Times

RIPE NCC:
YouTube reacted about 80 minutes after the Pakistan Telecom announcements, and all the major events finished after about two hours.

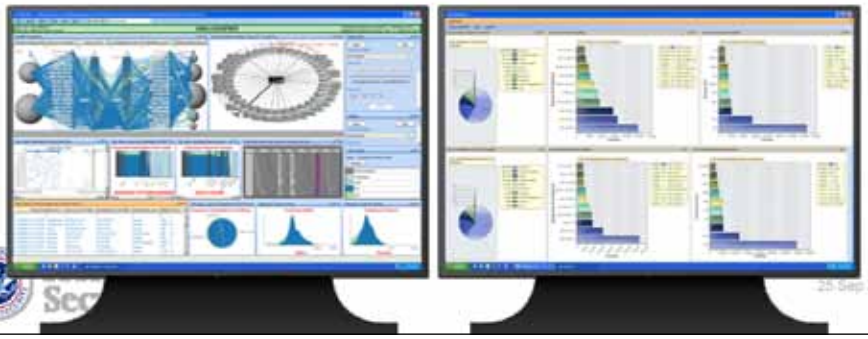
- Prefix Hijack Alert Sysem (PHAS)
  - Upgrading routing data collection infrastructure (RouteViews) to provide real-time (seconds) access to data that today is only available after several hours
  - Routing alert tool that provides hijack notification to network operation centers and personnel
    - http://phas.netsec.colostate.edu

Homeland Security

25 Sep 2008 24

Viz Toolkit for Network Analytics

- Current operations sees over 1B flows per day
- State of the art tool for network traffic analytics? MS Excel
- Need: Increase analysts' effectiveness and productivity
- Approach:
  - Present multiple perspectives to allow analysts to see data in new ways and put cyber attacks into context
  - Take advantage of powerful SiLK command line tools
- Working with US-CERT analysts for requirements and deployment

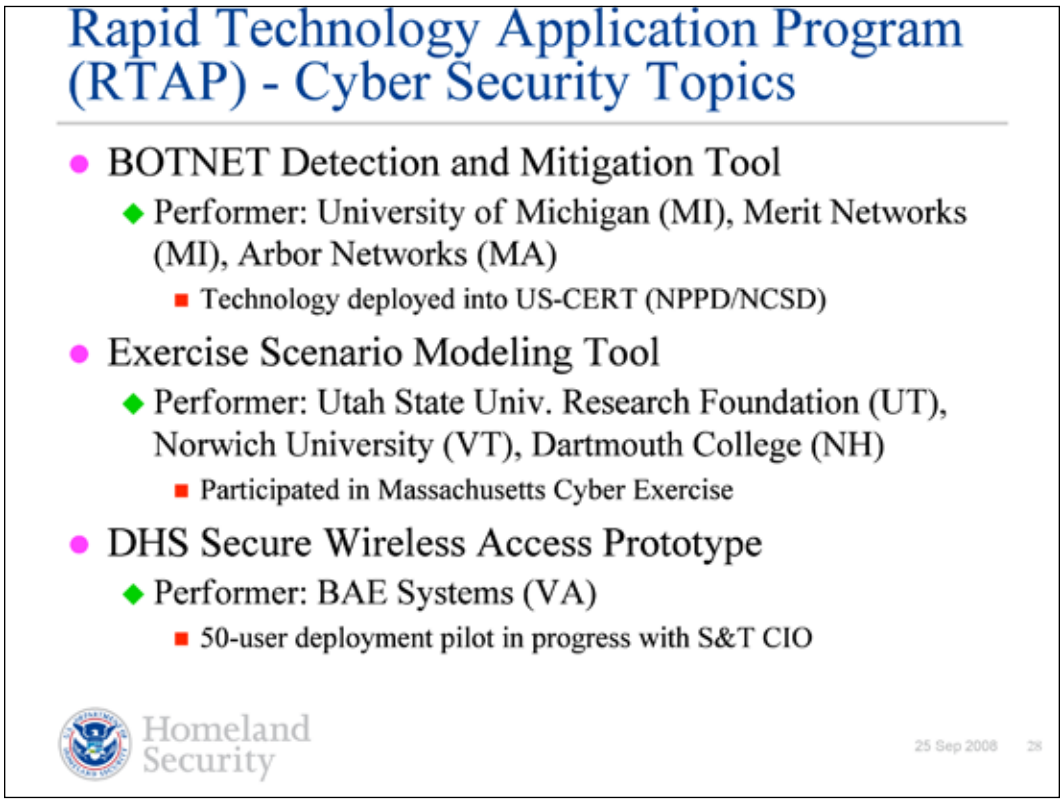


Other Activities:

SBIR
RTAP
Emerging Threats
Outreach
R&D Coordination

Homeland Security


Small Business Innovative Research (SBIR)
FY04
Cross-Domain Attack Correlation Technologies (2)
Real-Time Malicious Code Identification (2)
FY05
Hardware-assisted System Security Monitoring (4)
FY06
Network-based Boundary Controllers (3)
Botnet Detection and Mitigation (4)
FY07
Secure and Reliable Wireless Communication for Control Systems (2)
Homeland Security
25 Sep 2008
27


Rapid Technology Application Program (RTAP) - Cyber Security Topics
BOTNET Detection and Mitigation Tool
Performer: University of Michigan (MI), Merit Networks (MI), Arbor Networks (MA)
Technology deployed into US-CERT (NPPD/NCSD)
Exercise Scenario Modeling Tool
Performer: Utah State Univ. Research Foundation (UT), Norwich University (VT), Dartmouth College (NH)
Participated in Massachusetts Cyber Exercise
DHS Secure Wireless Access Prototype
Performer: BAE Systems (VA)
50-user deployment pilot in progress with S&T CIO
Homeland Security
25 Sep 2008
28

Emerging Threats

- Virtual Machine Environment - Detection and Escape Prevention
  - Vulnerability Discovery and Defenses for Virtual Machines
    - Results presented to commercial vendor and open source community
- Next Generation Crimeware Defenses
  - Research new techniques for defending against next generation malicious software
    - **Commercially available secure USB**
    - **1000+ user pilot in progress within DHS S&T**

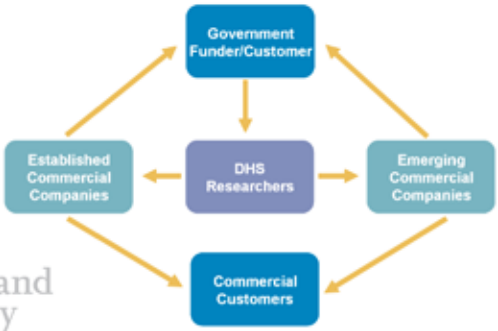
- Botnet Command & Control Detection and Mitigation
  - Examine defenses needed to counter new methods of Botnet C&C

Homeland Security

25 Sep 2008 29

Commercial Outreach Strategy

- Assist commercial companies in providing technology to DHS and other government agencies
  - Emerging Security Technology Forum (ESTF)
- Assist DHS S&T-funded researchers in transferring technology to larger, established security technology companies
  - **System Integrator Forum (Feb. 21, 2008)**
- Partner with the venture capital community to transfer technology to existing portfolio companies, or to create new ventures
  - **Cyber Entrepreneurs Workshop (Mar. 11, 2008)**



Homeland Security

25 Sep 2008 30

System Integrator Forum 2008

- IronKey, Palo Alto, CA
  - Secure USB Token
- HBGary, Chevy Chase, MD
  - Malware Discovery Tool
- Grammatech, Ithaca, NY
  - Software Analysis (Binary and Source)
- George Mason Univ, Fairfax, VA
  - Network Vulnerability Analysis/Discovery
- Endeavor Systems, Arlington, VA
  - Pattern Recognition and Signature Analysis

- 2008 SIF – February 21 in WDC (see website)
- 2009 SIF – Planning in progress; Want an invitation? Let me know

Homeland Security

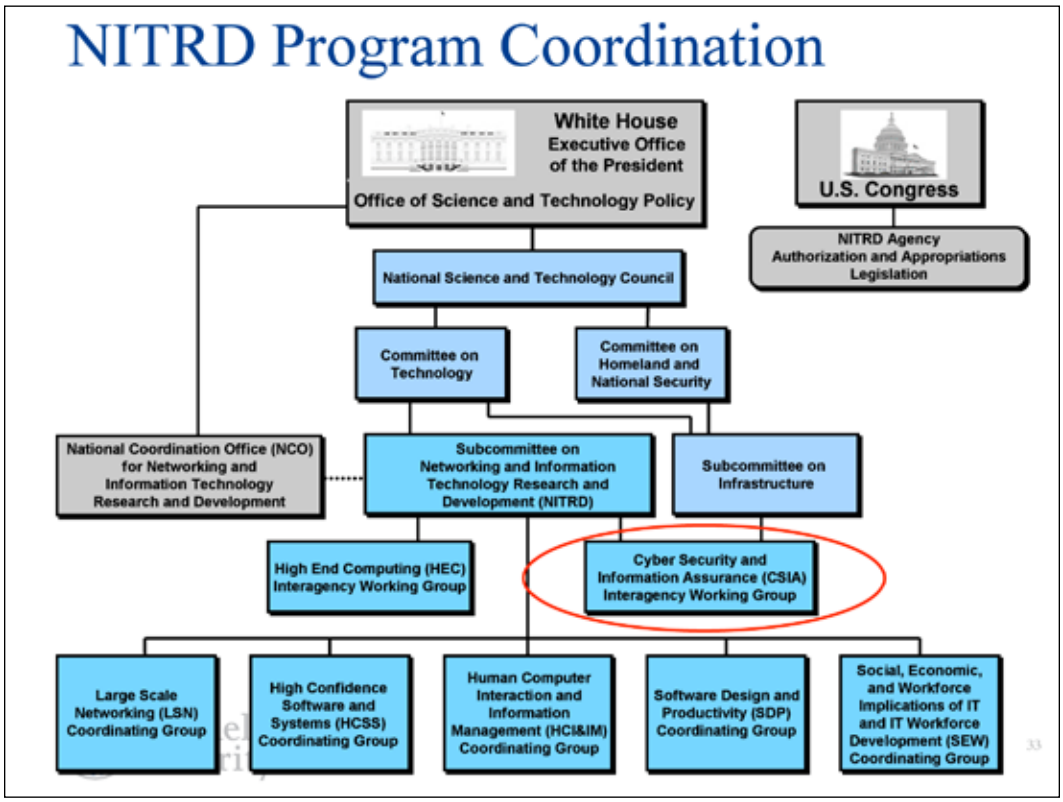
25 Sep 2008 31

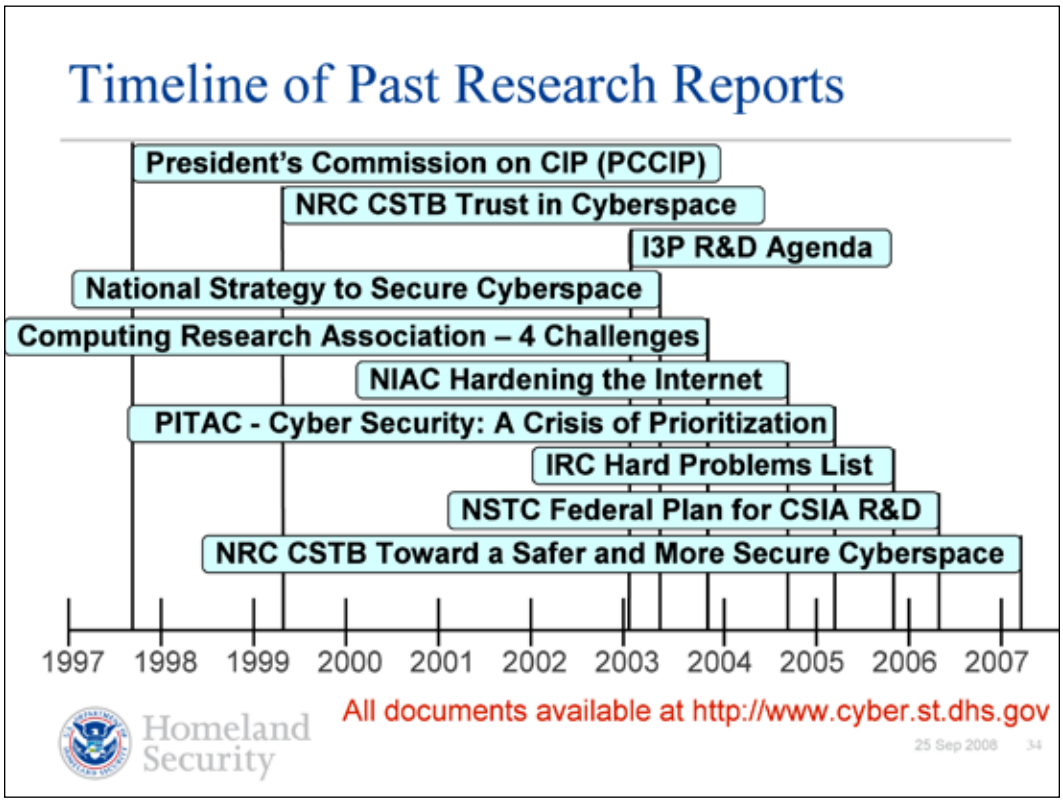
IT Security Entrepreneur Forum (ITSEF)

- 2007 Topics
  - How to Optimize Having the Government as Your Partner
  - The Risks and Rewards of Selling to the Government
  - Navigating the Government Procurement Process from A to Z
- 2008 Topics
  - Systems Integrators and Entrepreneurial Activities
  - What does it take to get VC Funding?
  - Achieving Value & Liquidity in IT Security: A Wall Street Perspective
- 2009 ITSEF – March 18 @ Stanford
  - http://www.publicprivatepartnerships.org

Homeland Security

25 Sep 2008 32


NITRD Program Coordination
White House
Executive Office of the President
Office of Science and Technology Policy
U.S. Congress
NITRD Agency Authorization and Appropriations Legislation
National Science and Technology Council
Committee on Technology
Committee on Homeland and National Security
National Coordination Office (NCO) for Networking and Information Technology Research and Development
Subcommittee on Networking and Information Technology Research and Development (NITRD)
Subcommittee on Infrastructure
High End Computing (HEC) Interagency Working Group
Cyber Security and Information Assurance (CSIA) Interagency Working Group
Large Scale Networking (LSN) Coordinating Group
High Confidence Software and Systems (HCSS) Coordinating Group
Human Computer Interaction and Information Management (HCI&IM) Coordinating Group
Software Design and Productivity (SDP) Coordinating Group
Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) Coordinating Group


Timeline of Past Research Reports
President's Commission on CIP (PCCIP)
NRC CSTB Trust in Cyberspace
I3P R&D Agenda
National Strategy to Secure Cyberspace
Computing Research Association – 4 Challenges
NIAC Hardening the Internet
PITAC - Cyber Security: A Crisis of Prioritization
IRC Hard Problems List
NSTC Federal Plan for CSIA R&D
NRC CSTB Toward a Safer and More Secure Cyberspace
1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007
Homeland Security
All documents available at http://www.cyber.st.dhs.gov
25 Sep 2008 34

Tackling Cyber Security R&D Challenges: *Not* Business as Usual

- Key people in WDC now paying attention
- Close coordination with other Federal agencies
- Outreach to communities outside of the Federal government
  - Building public-private partnerships (the industry-government *dance* is an interesting new tango)
- Need a stronger emphasis on technology diffusion and technology transfer
- Migration paths to a more secure infrastructure
- Awareness of economic realities

Homeland Security

25 Sep 2008 35

Summary

- DHS has a difficult mission– many supporters, many critics, continues to make improvements
- DHS S&T is moving forward with an aggressive cyber security research agenda
  - Working with the community to solve the cyber security problems of our current (and future) infrastructure
  - Working with academe and industry to improve research tools and datasets
  - Looking at future R&D agendas with the most impact for the nation

Homeland Security

25 Sep 2008 36


Douglas Maughan, Ph.D.
Program Manager, CCI
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170
U.S. DEPARTMENT OF HOMELAND SECURITY
For more information, visit
http://www.cyber.st.dhs.gov
Homeland Security
25 Sep 2008
37

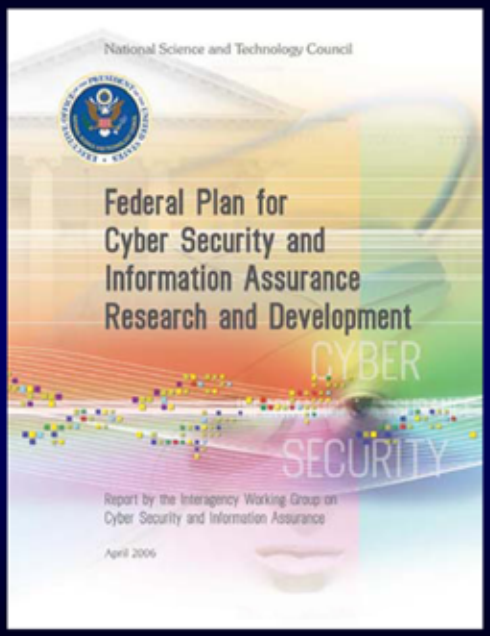
Presentation – Dr. Chris Greer

2008 Research and Development Exchange Workshop

President's National Security Telecommunications Advisory Committee

September 24-26, 2008

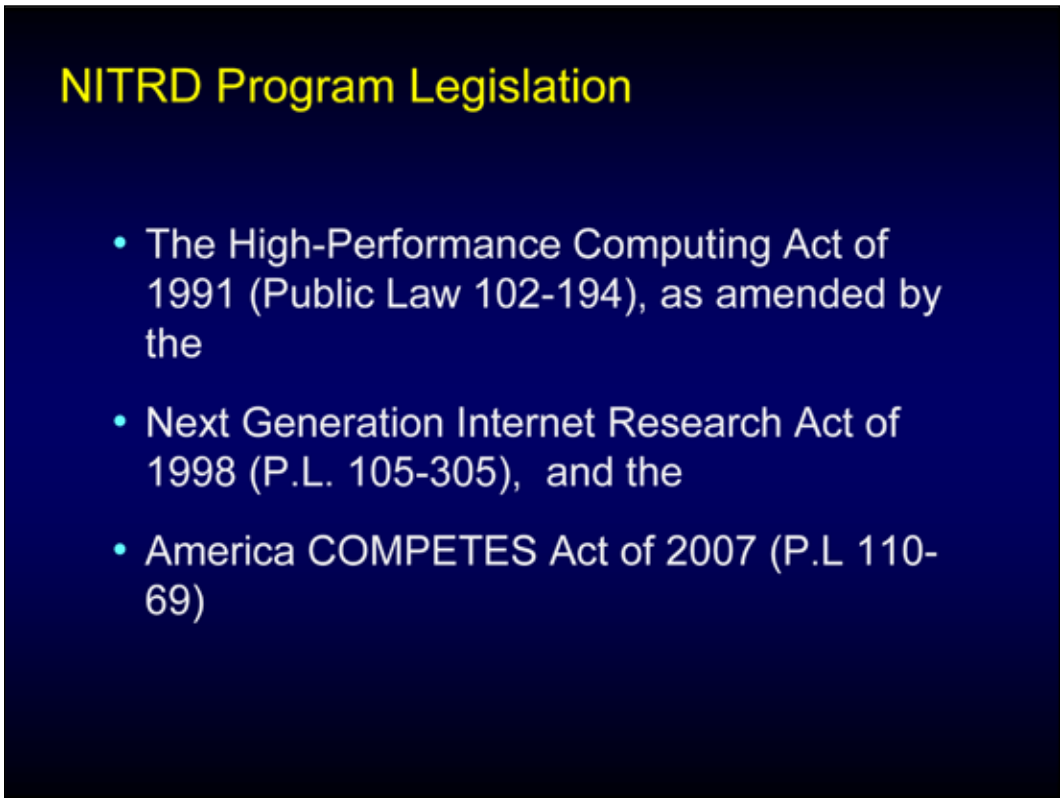
Chris Greer
Director, US National Coordination Office
Networking and Information Technology Research and Development Program



The Nation's information technology (IT) infrastructure … has become indispensable to public- and private-sector activities throughout our society and around the globe.

Safeguarding the Nation's IT infrastructure and critical infrastructure sectors for the future is a matter of national and homeland security.


Acronyms:
NITRD
Networking and Information Technology Research and Development Program
NCO
National Coordination Office
CSIA
Cybersecurity and Information Assurance Working Group
CNCI
Comprehensive National Cybersecurity Initiative


NITRD Program Legislation
• The High-Performance Computing Act of 1991 (Public Law 102-194), as amended by the
• Next Generation Internet Research Act of 1998 (P.L. 105-305), and the
• America COMPETES Act of 2007 (P.L 110-69)

NITRD Responsibilities

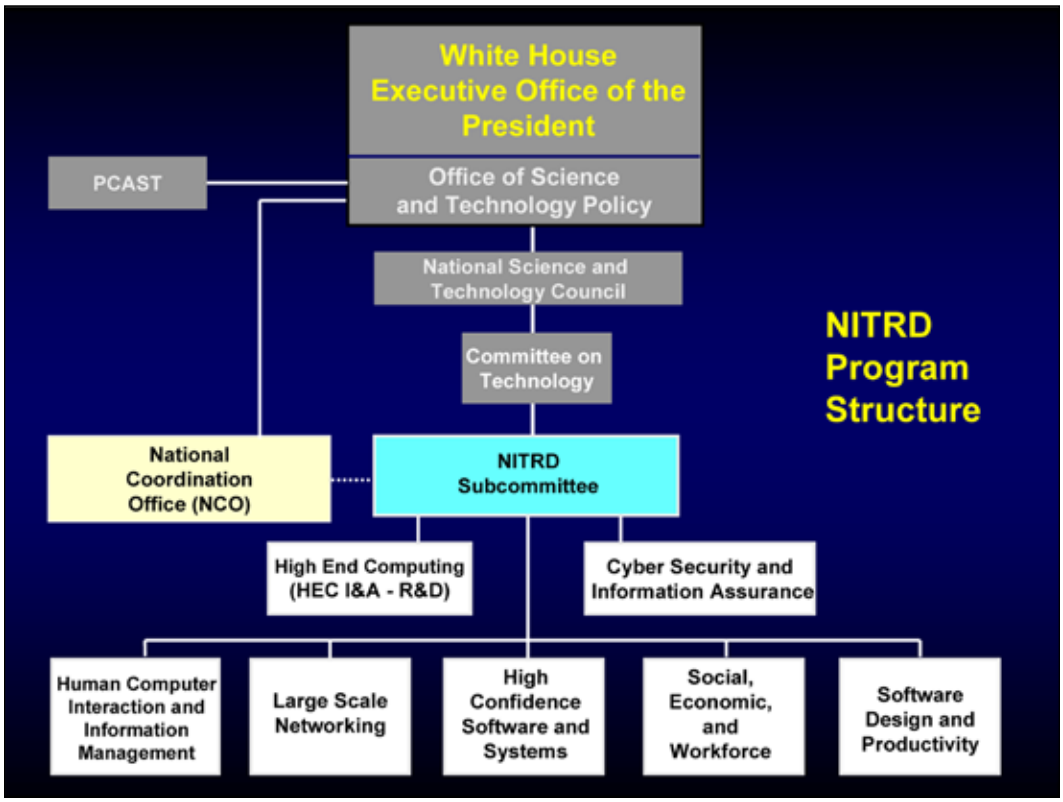
- Improved security for computing and networking systems in Federal and other realms.
- Long-term basic and applied research on high-performance computing, networking systems, and related software.
- Access by the U.S. research community to high-performance computing and networking systems.
- NIT capabilities to address Grand Challenges, increased software availability, productivity, capability, security, portability, and reliability; and mathematical modeling and algorithms for all fields of science and engineering.
- Education and training in software engineering, computer science, cyber security, applied mathematics, library and information science, and computational science.

NITRD Responsibilities

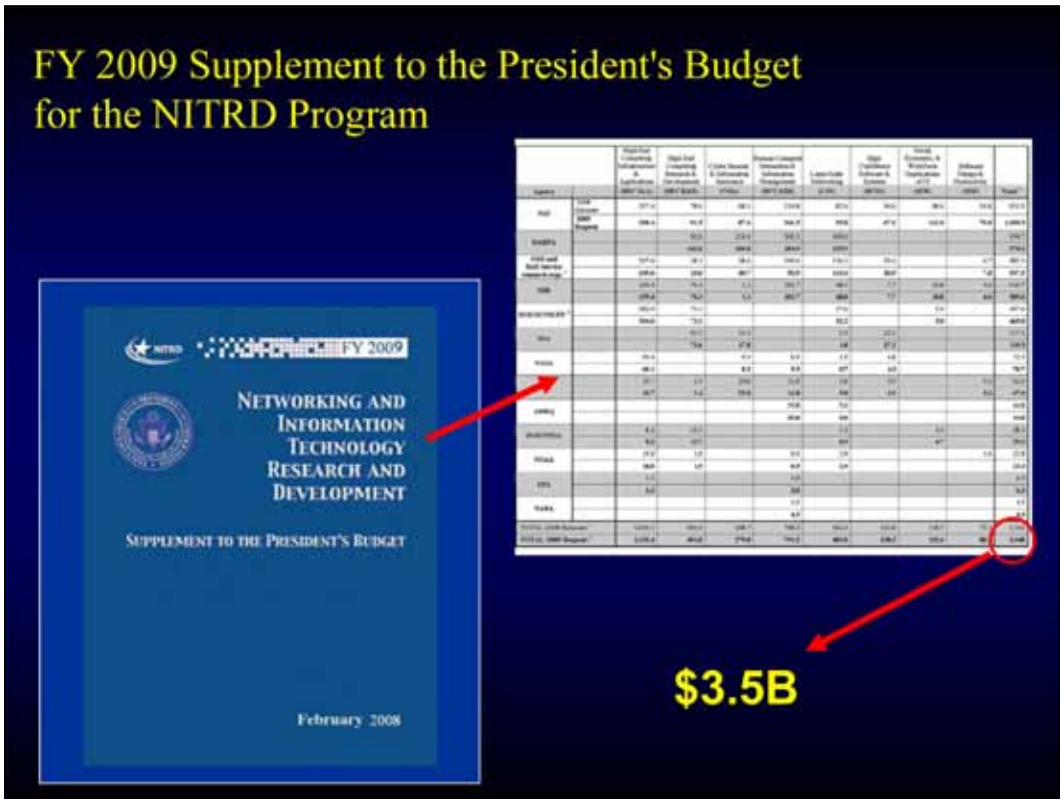
- Improved security for computing and networking systems in Federal and other realms.
- Long-term basic and applied research on high-performance computing, networking systems, and related software.
- Education and training in software engineering, computer science, cyber security, applied mathematics, library and information science, and computational science.

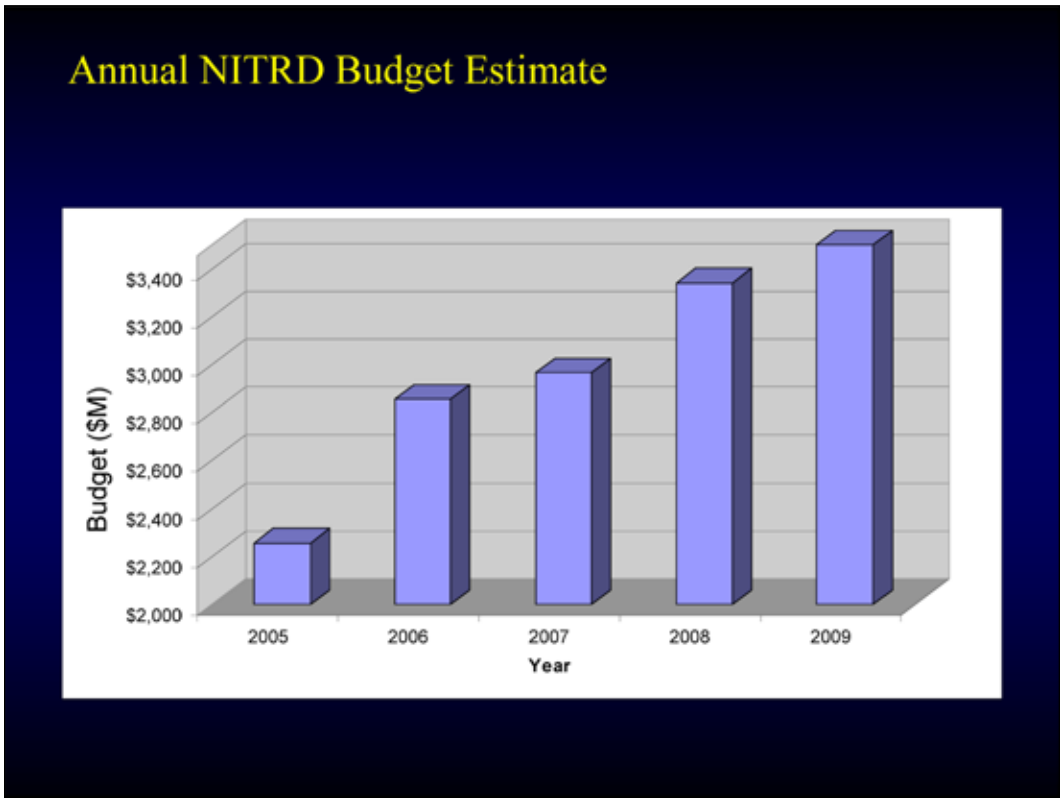
NITRD Mission

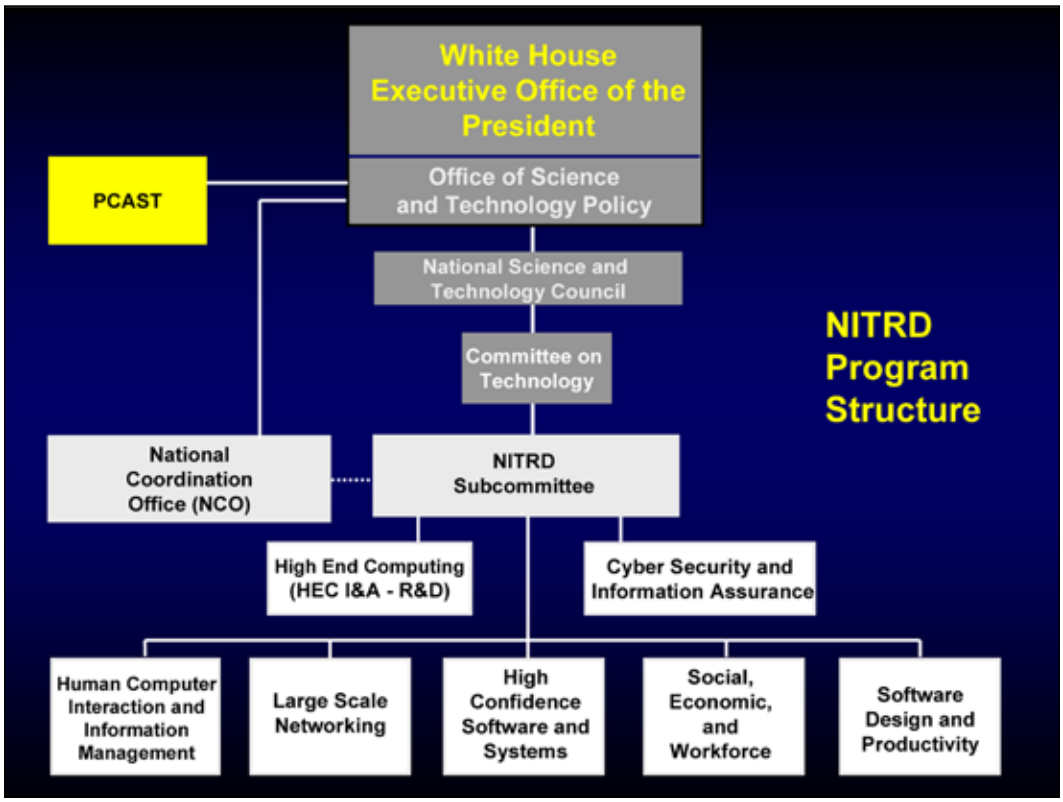
to empower individuals and organizations, promote innovation and progress, provide for security, and improve the quality of life by accelerating research, development, and educational advances in networking and information technologies through coordination, joint planning, partnerships, and information sharing across government, academic, non-profit, and commercial sectors, national and international.




AHRQ Agency for Healthcare Research and Quality
DARPA Defense Advanced Research Projects Agency
DOE/NNSA Department of Energy - National Nuclear Security Agency
DOE/SC Department of Energy - Mathematical, Information, and Computational Science Division
EPA Environmental Protection Agency
NARA National Archives and Records Administration
NASA National Aeronautics and Space Administration
NIH National Institutes of Health
NIST National Institute of Standards and Technology
NOAA National Oceanic and Atmospheric Administration
NSA National Security Agency
NSF National Science Foundation
OSD and DoD Service research organizations, Office of the Deputy, Under Secretary of Defense (Science and Technology)


FY 2009 Supplement to the President's Budget for the NITRD Program
FY 2009
Networking and Information Technology Research and Development
Supplement to the President's Budget
February 2008
$3.5B


Annual NITRD Budget Estimate
Budget ($M)
$3,400
$3,200
$3,000
$2,800
$2,600
$2,400
$2,200
$2,000
2005
2006
2007
2008
2009
Year


White House
Executive Office of the President
PCAST
Office of Science and Technology Policy
National Science and Technology Council
Committee on Technology
NITRD Program Structure
National Coordination Office (NCO)
NITRD Subcommittee
High End Computing (HEC I&A - R&D)
Cyber Security and Information Assurance
Human Computer Interaction and Information Management
Large Scale Networking
High Confidence Software and Systems
Social, Economic, and Workforce
Software Design and Productivity

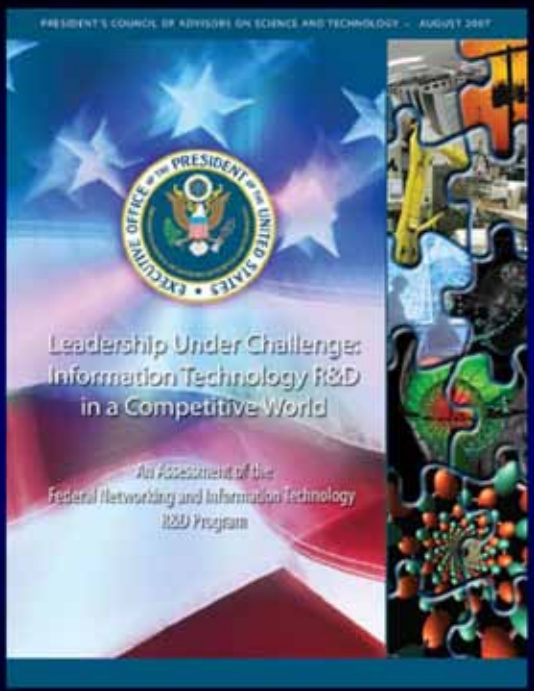
Under Executive order 13226, PCAST ..

… enables the President to receive advice from the private sector and academic community on technology, scientific research priorities, and math and science education.

… is composed of distinguished individuals appointed by the President and drawn from industry, education, and research institutions, and other nongovernmental organizations.

PCAST Assessment of the NITRD Program

August, 2007



www.ostp.gov/cs/pcast

NITRD Program Assessment

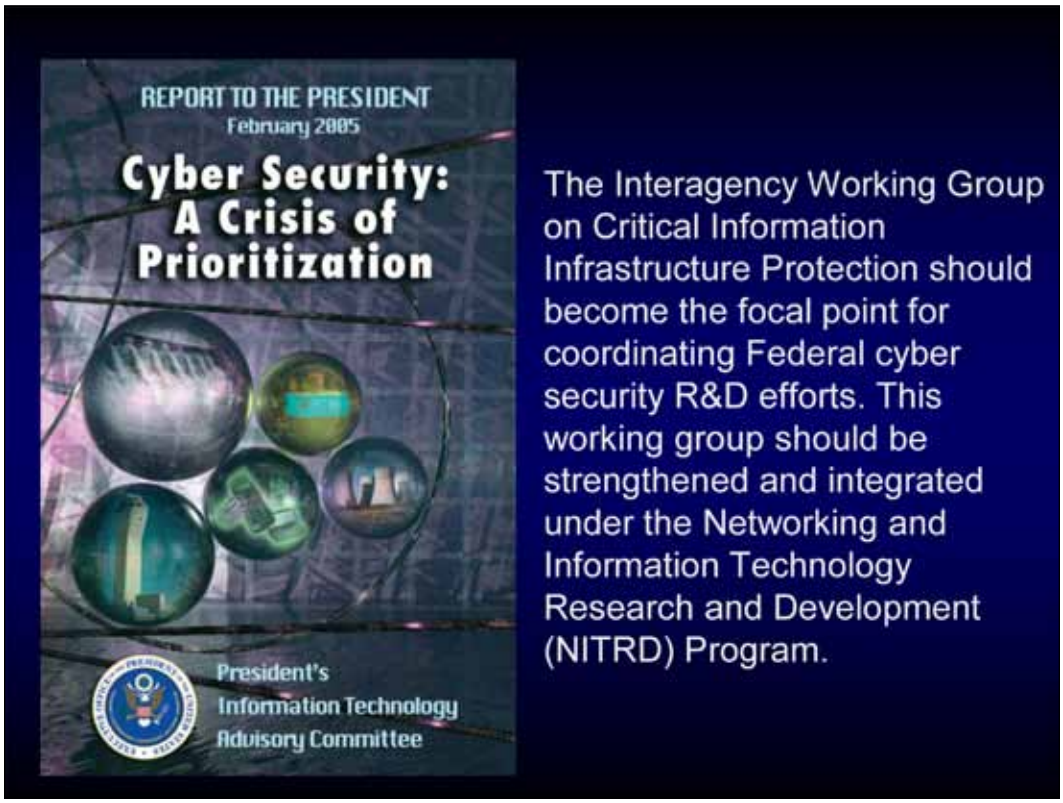
- Findings
  - In general, the NITRD Program has effectively balanced statutory mandates and agency mission requirements
  - However, the NITRD Program's *current coordination processes are inadequate* to meet anticipated national needs and to maintain U.S. leadership in a globally competitive world
- Recommendations
  - The NSTC's NITRD Subcommittee should *develop and maintain a strategic plan and public technology R&D plans* for the NITRD Program that includes an overarching vision of challenges and approaches
  - This strategic planning process should hold annual planning and review meetings with broad agency participation

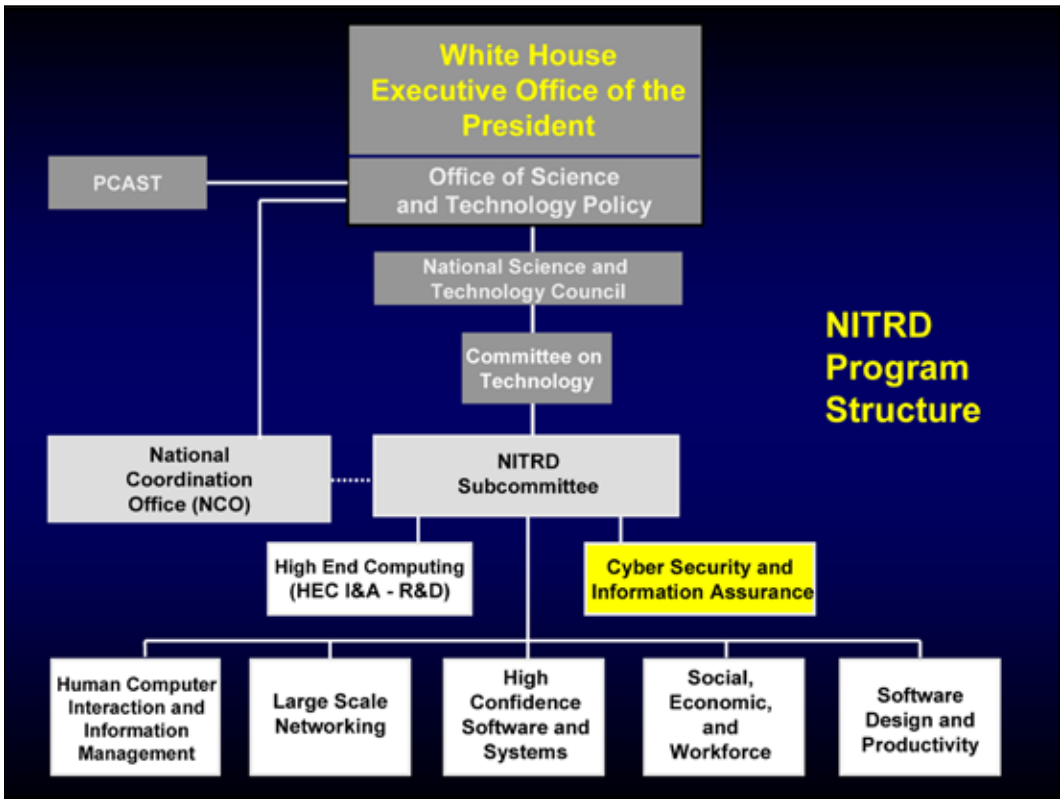
NITRD Strategic Planning Timeline

RFI — Open Workshop — Public Comments

Strategic Framework — Draft Text — Final Text

www.nitrd.gov


REPORT TO THE PRESIDENT
February 2005
Cyber Security: A Crisis of Prioritization
President's Information Technology Advisory Committee
The Interagency Working Group on Critical Information Infrastructure Protection should become the focal point for coordinating Federal cyber security R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.


White House Executive Office of the President
PCAST
Office of Science and Technology Policy
National Science and Technology Council
Committee on Technology
NITRD Program Structure
National Coordination Office (NCO)
NITRD Subcommittee
High End Computing (HEC I&A - R&D)
Cyber Security and Information Assurance
Human Computer Interaction and Information Management
Large Scale Networking
High Confidence Software and Systems
Social, Economic, and Workforce
Software Design and Productivity

CSIA Scope

- Security of computer-based systems that support critical infrastructures and other vital Federal missions
- CSIA R&D for protection of the Nation's information technology infrastructure
- Close communication and liaison among the CSIA agencies, academia, and industry to address CSIA R&D needs

CIA Central Intelligence Agency

DARPA Defense Advanced Research Projects Agency

DoE Department of Energy

DHS Department of Homeland Security – National Communications System, National Cyber Security Division, Science and Technology

DoJ Department of Justice

DoS Department of State

DoT FAA, Research and Innovate Technology Administration

NASA National Aeronautics and Space Administration

NIH National Institutes of Health

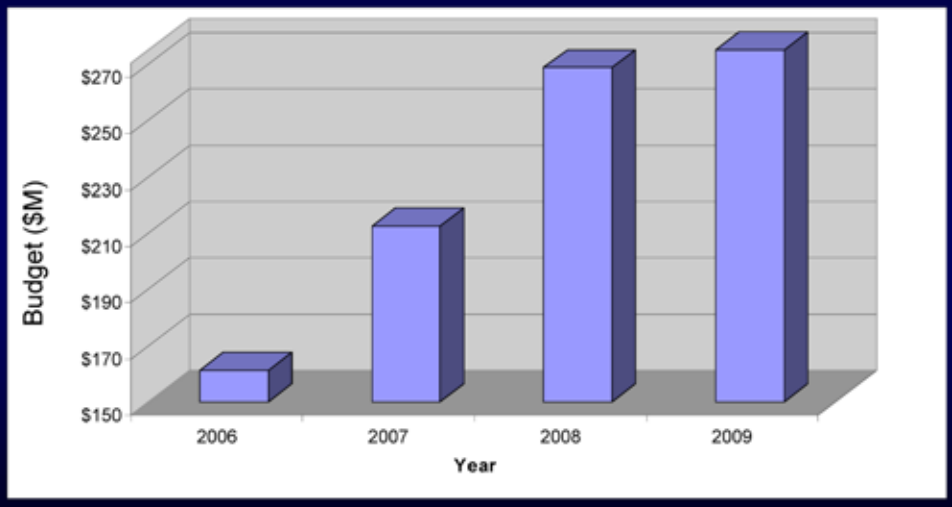
NIST National Institute of Standards and Technology

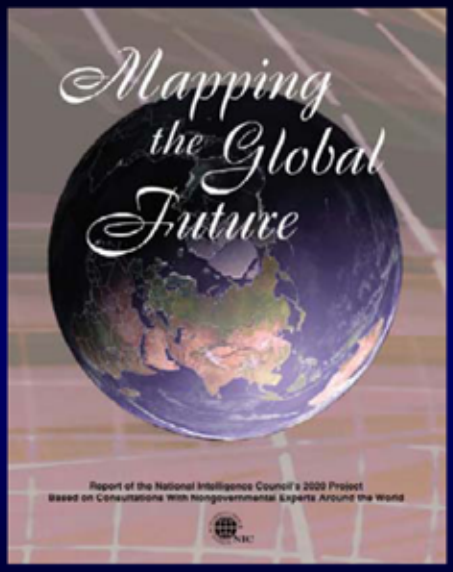
NSA National Security Agency

NSF National Science Foundation

OSD and DoD Service research organizations, Office of the Deputy, Under Secretary of Defense (Science and Technology)

CSIA Annual Budget Estimate



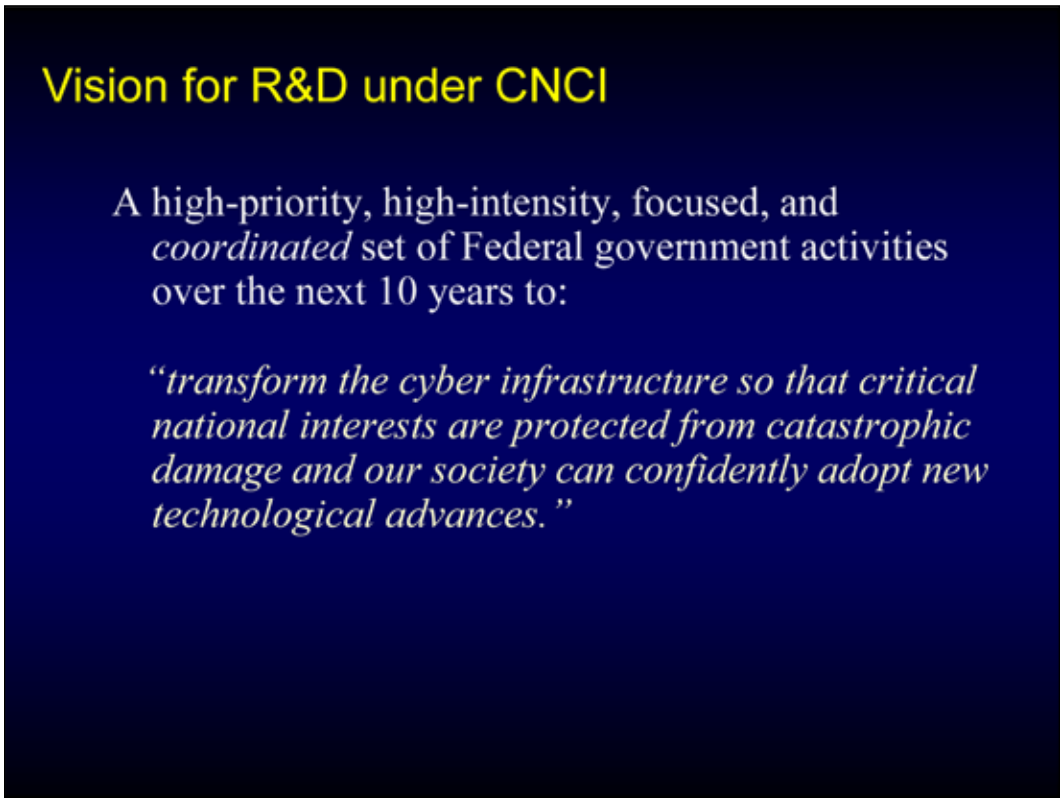


"Over the next 15 years, a growing range of actors, including terrorists, may acquire and develop capabilities to conduct both physical and cyber attacks against nodes of the world's information infrastructure …

…The ability to respond to such attacks will require critical technology to close the gap between attacker and defender."

National Intelligence Council
2020 Project


Comprehensive National
Cybersecurity Initiative(CNCI):
R&D Coordination and Leap-Ahead
Activities

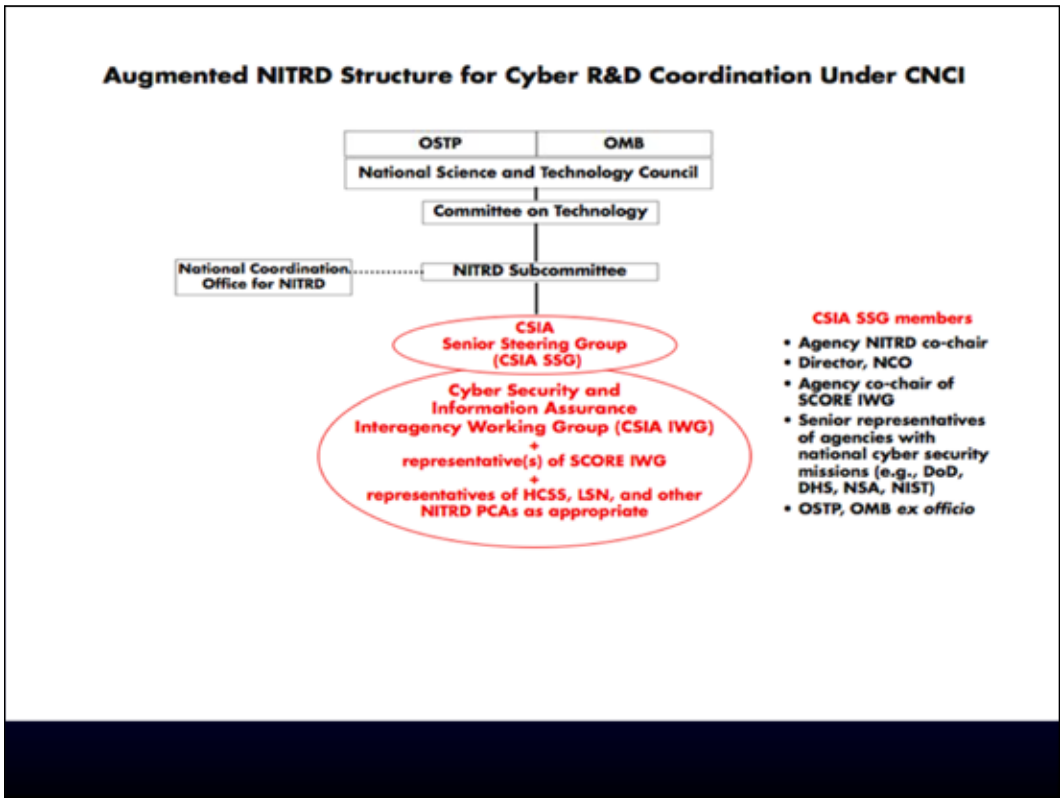

Vision for R&D under CNCI
A high-priority, high-intensity, focused, and
coordinated set of Federal government activities
over the next 10 years to:
"transform the cyber infrastructure so that critical
national interests are protected from catastrophic
damage and our society can confidently adopt new
technological advances."

Principles for Multidimensional Cyber R&D:

1) Improve synergy between classified and unclassified Federal research
2) Enable a broad multidisciplinary, multisector effort
3) Prioritize research needs and involve the private sector in determining appropriate roles and investment strategies
4) Enable agencies to leverage resources
5) Maximize intellectual capital
6) Exploit the full range of existing R&D models and develop new, streamlined approaches for high-risk/high-payoff R&D

CNCI Coordination Founded on NITRD :

- NITRD's advantages
  - Provides the foundation for a rapid launch of CNCI coordination activities
  - 17-year history, arguably most successful formal interagency research coordination activity
  - Substantial institutional knowledge about multi-agency coordination
  - Established support mechanisms to facilitate coordination processes
  - Represents full range of Federal R&D agencies in the areas relevant to cyber security technologies
  - Reflects multidisciplinary and multisector principles
  - Engages managers and researchers across many disciplines in the agencies, national laboratories, academia, and industry
  - NITRD participants are among those whose science and technology expertise and agency experience will be needed


Augmented NITRD Structure for Cyber R&D Coordination Under CNCI
OSTP
OMB
National Science and Technology Council
Committee on Technology
National Coordination Office for NITRD
NITRD Subcommittee
CSIA Senior Steering Group (CSIA SSG)
Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)
+
representative(s) of SCORE IWG
+
representatives of HCSS, LSN, and other NITRD PCAs as appropriate
CSIA SSG members
• Agency NITRD co-chair
• Director, NCO
• Agency co-chair of SCORE IWG
• Senior representatives of agencies with national cyber security missions (e.g., DoD, DHS, NSA, NIST)
• OSTP, OMB ex officio


THE NATIONAL STRATEGY TO
SECURE CYBERSPACE
FEBRUARY 2003
The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership. The federal government invites the creation of, and participation in, public-private partnerships to implement this strategy. Only by acting together can we build a more secure future in cyberspace.


Contact:
greer@nitrd.gov

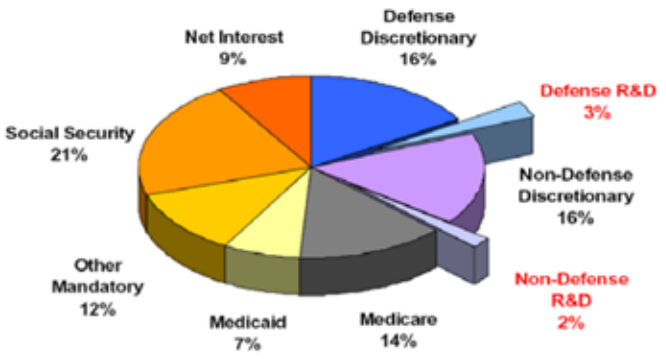
Plenary Address – Ambassador Richard Russell

NSTAC R&D Exchange

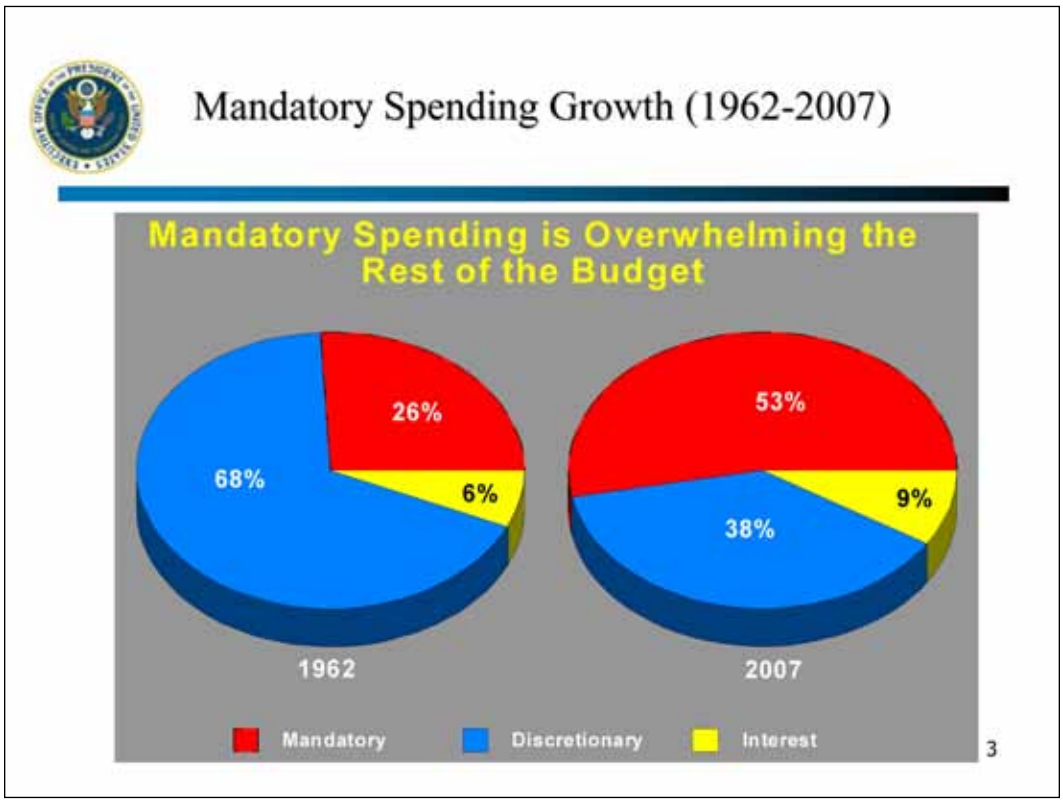
Ambassador Richard M. Russell

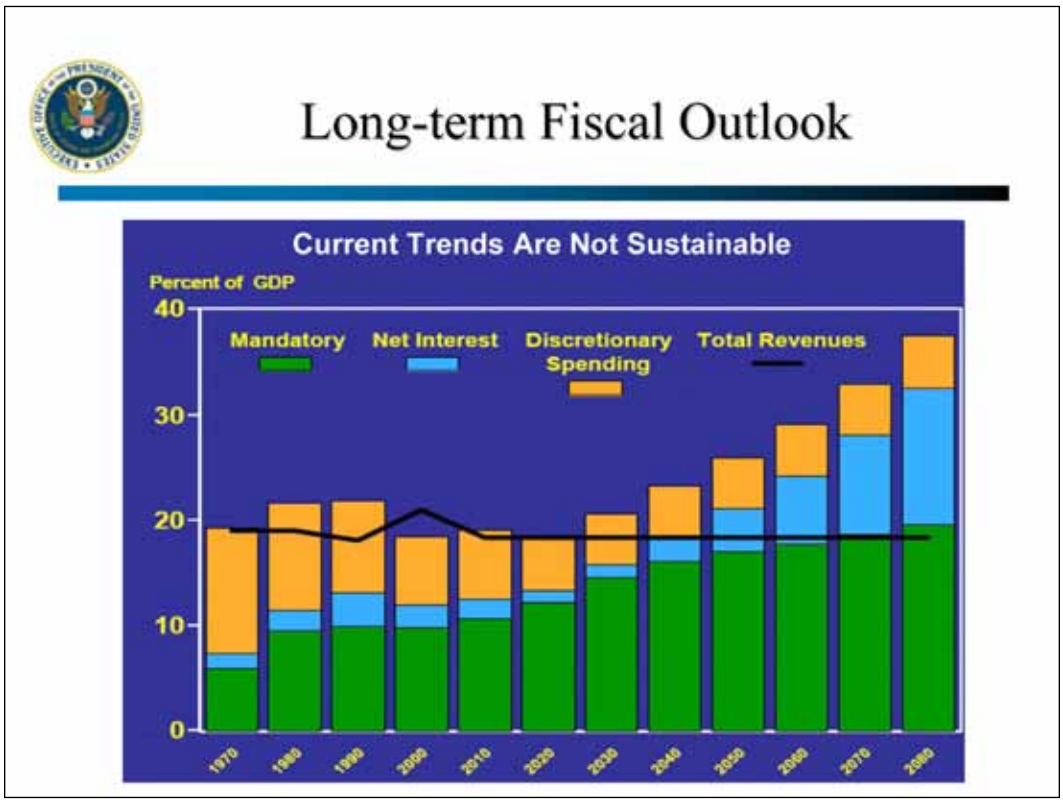
Associate Director and Deputy Director for Technology
Office of Science and Technology Policy
Executive Office of the President

President's FY 2009 Budget Request ($3.1 Trillion in Outlays)



R&D = 15% of discretionary spending


Mandatory Spending Growth (1962-2007)
Mandatory Spending is Overwhelming the Rest of the Budget
26%
68%
6%
53%
38%
9%
1962
2007
Mandatory
Discretionary
Interest
3

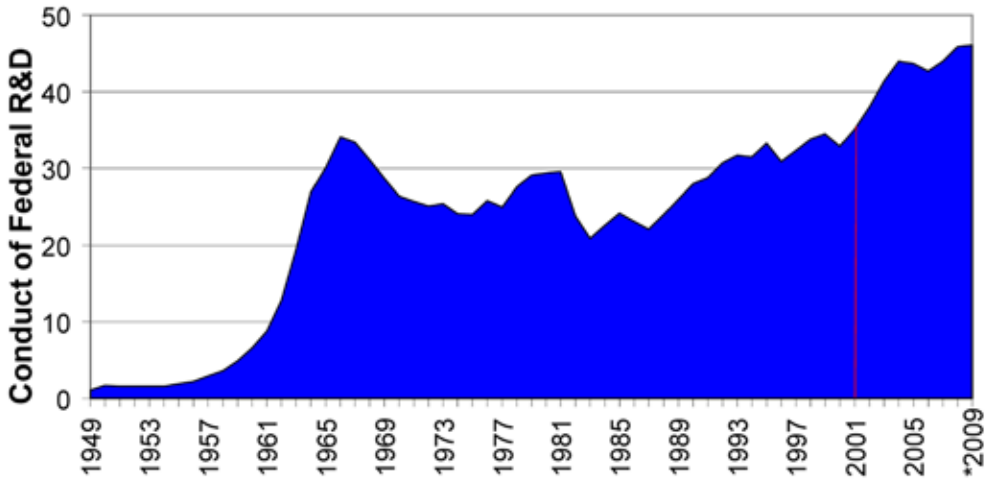

Long-term Fiscal Outlook
Current Trends Are Not Sustainable
Percent of GDP
40
30
20
10
0
Mandatory
Net Interest
Discretionary Spending
Total Revenues
1970
1980
1990
2000
2010
2020
2030
2040
2050
2060
2070
2080

FY2009 R&D Highlights

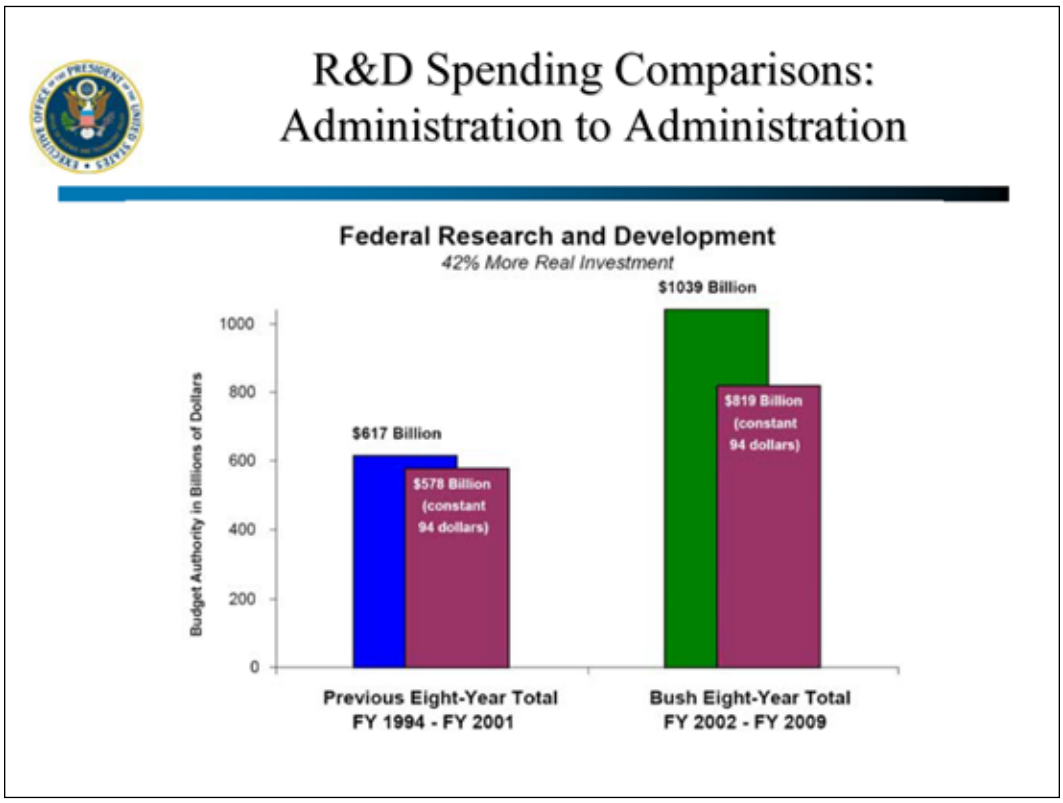
- In the 2009 Budget, total Federal R&D is $147 billion, an increase of $3.9 billion (three percent) over FY2008.
- This represents a 61% increase compared to 2001's $91.3 billion. R&D accounts for one of every seven discretionary dollars.
- Non-defense R&D increases six percent in the 2009 Budget over FY 2008, compared to less than one percent for overall non-security discretionary spending.

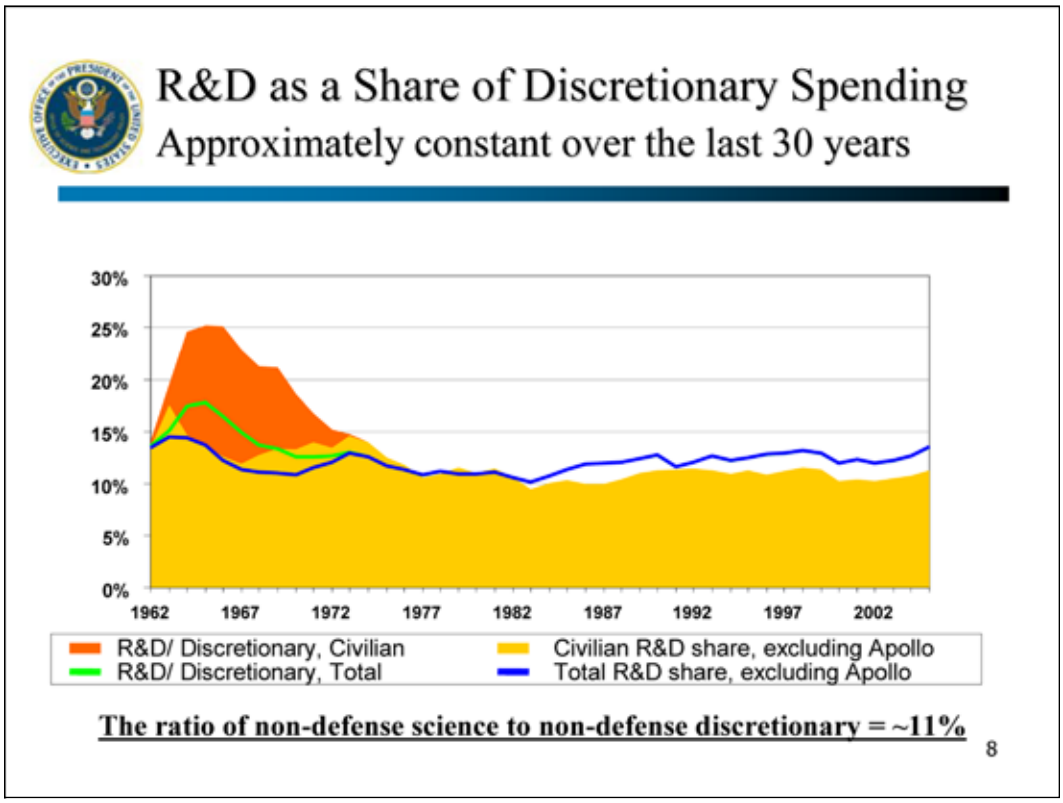
5

Federal Non-Defense R&D Spending
(Outlays in billions, constant 2000 dollars)



6


R&D Spending Comparisons:
Administration to Administration
Federal Research and Development
42% More Real Investment
$1039 Billion
$819 Billion
(constant
94 dollars)
$617 Billion
$578 Billion
(constant
94 dollars)
Budget Authority in Billions of Dollars
1000
800
600
400
200
0
Previous Eight-Year Total
FY 1994 - FY 2001
Bush Eight-Year Total
FY 2002 - FY 2009


R&D as a Share of Discretionary Spending
Approximately constant over the last 30 years
30%
25%
20%
15%
10%
5%
0%
1962
1967
1972
1977
1982
1987
1992
1997
2002
R&D/ Discretionary, Civilian
R&D/ Discretionary, Total
Civilian R&D share, excluding Apollo
Total R&D share, excluding Apollo
The ratio of non-defense science to non-defense discretionary = ~11%
8

Basic Research Impact on Innovation

Prioritizing Research

"Tonight I announce an American Competitiveness Initiative…This funding will support the work of America's most creative minds as they explore promising areas such as nanotechnology, supercomputing, and alternative energy sources."

-- President George W. Bush (2006 State of the Union Address)

American Competitiveness Initiative

$136B over 10 years

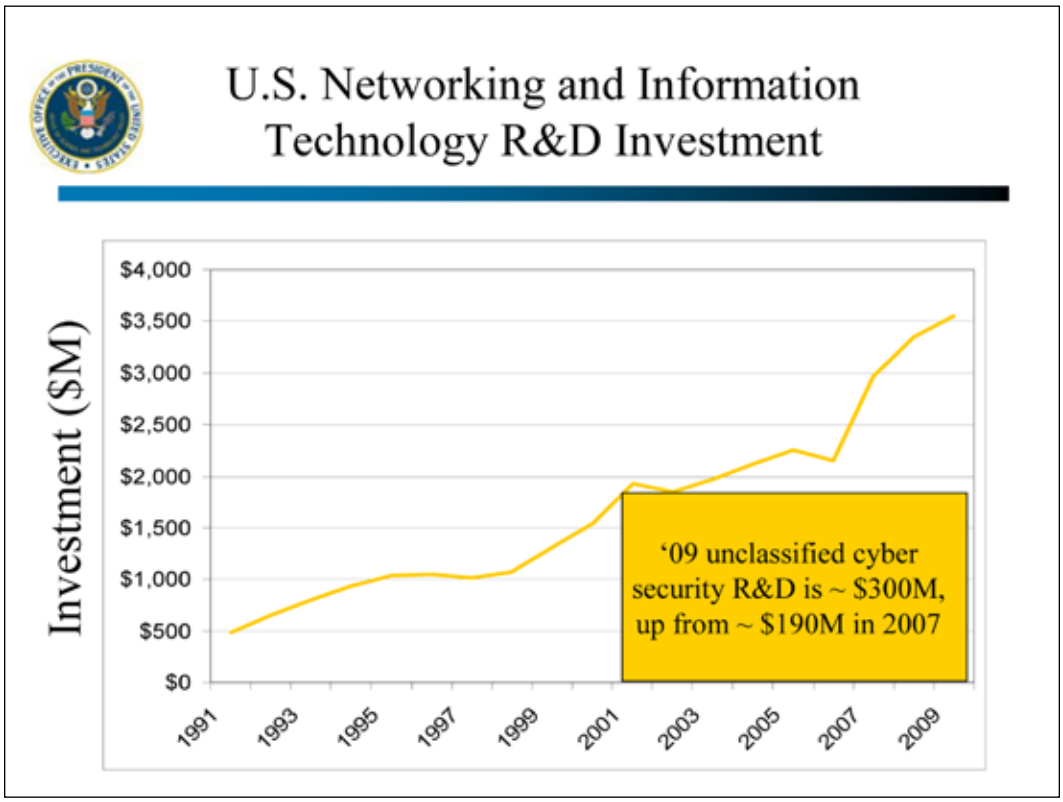
- Funding long-term, high-risk research is a federal responsibility.
- Areas of science most likely to contribute to long-term economic competitiveness should receive priority.
- The current level of funding for research in the physical sciences is too low in many agencies.

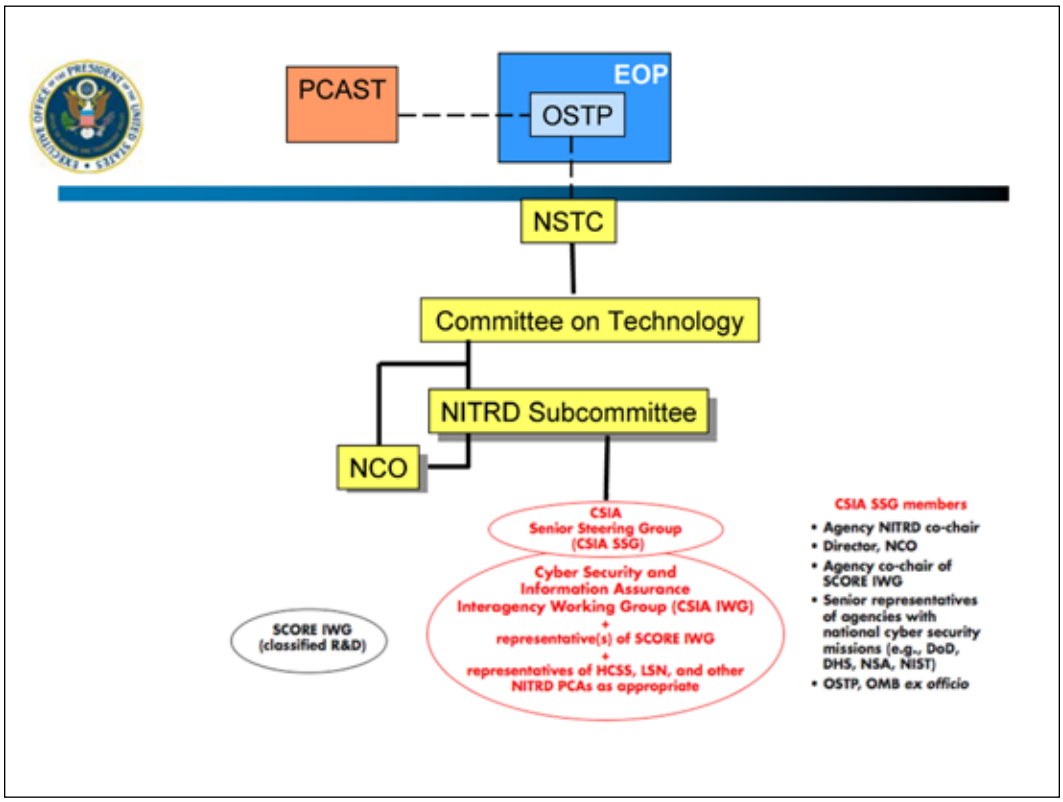
11

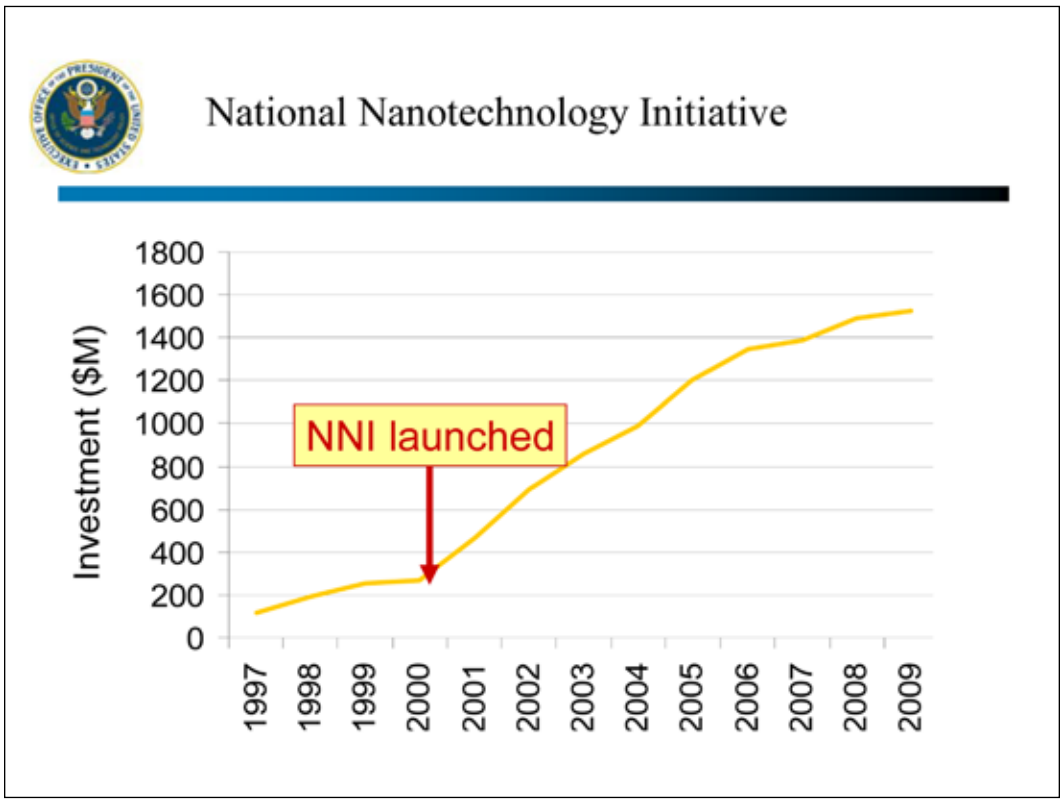
ACI Supports High Impact Research

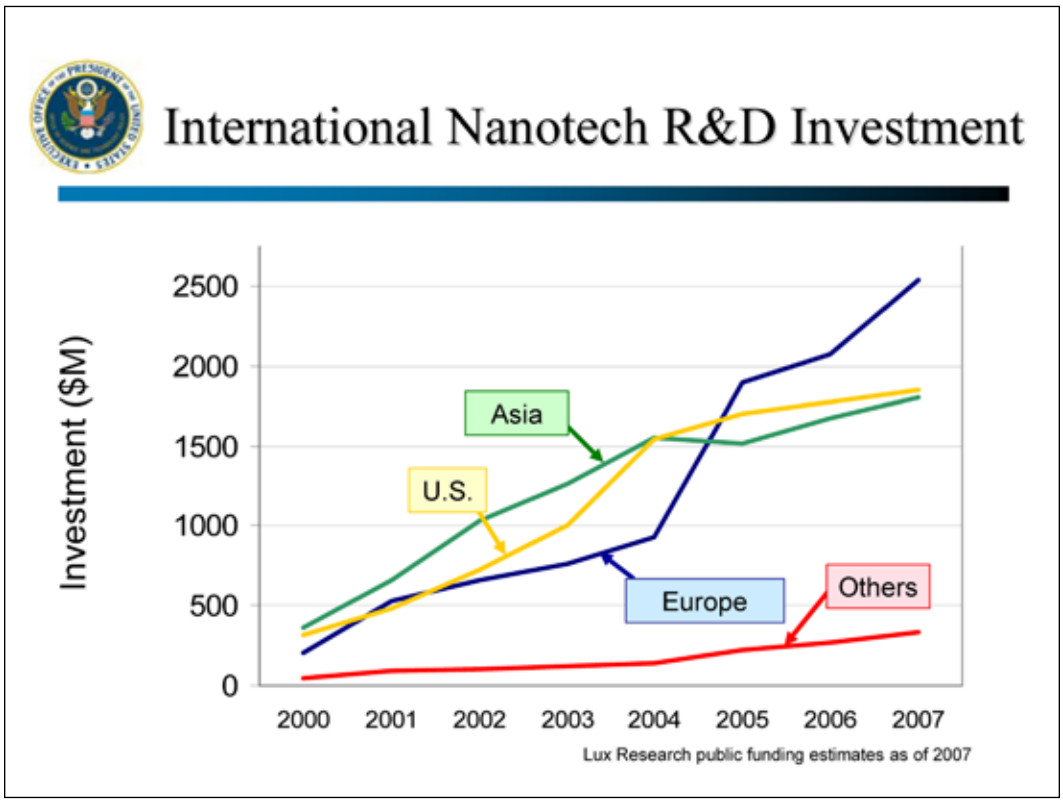
Goals for ACI Research

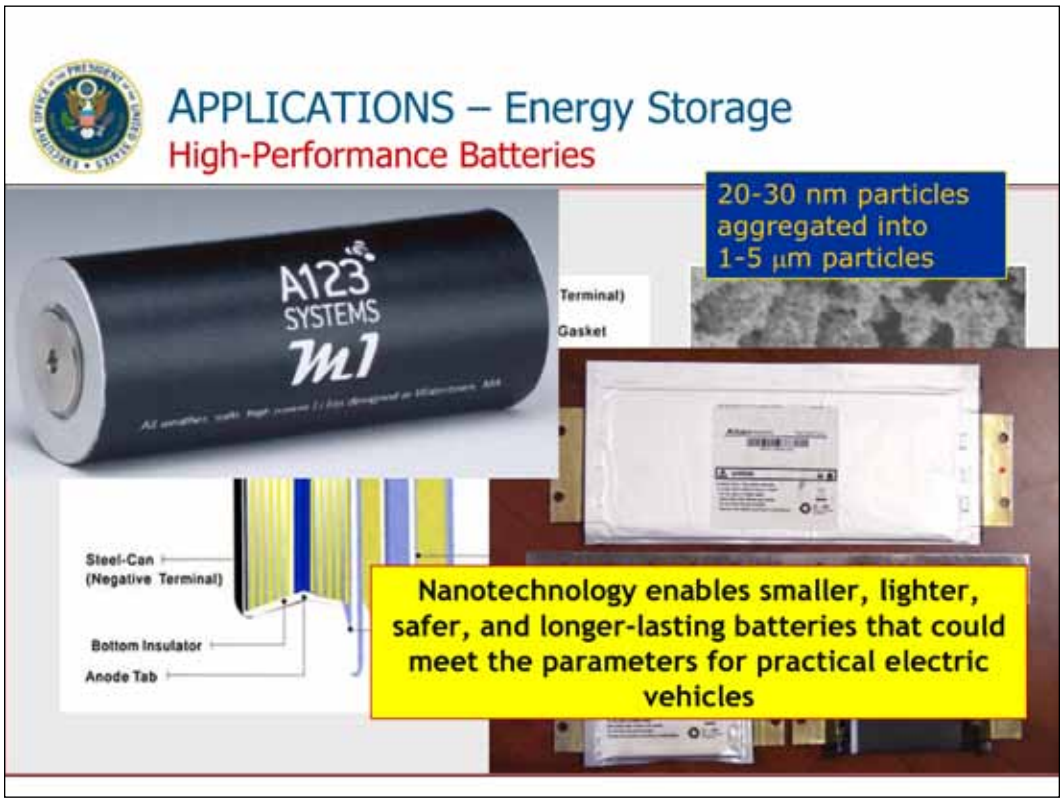
Cyber Security: "Addressing gaps and needs in cyber security and information assurance to protect our IT-dependent economy from both deliberate and unintentional disruption, and to lead the world in intellectual property protection and control"

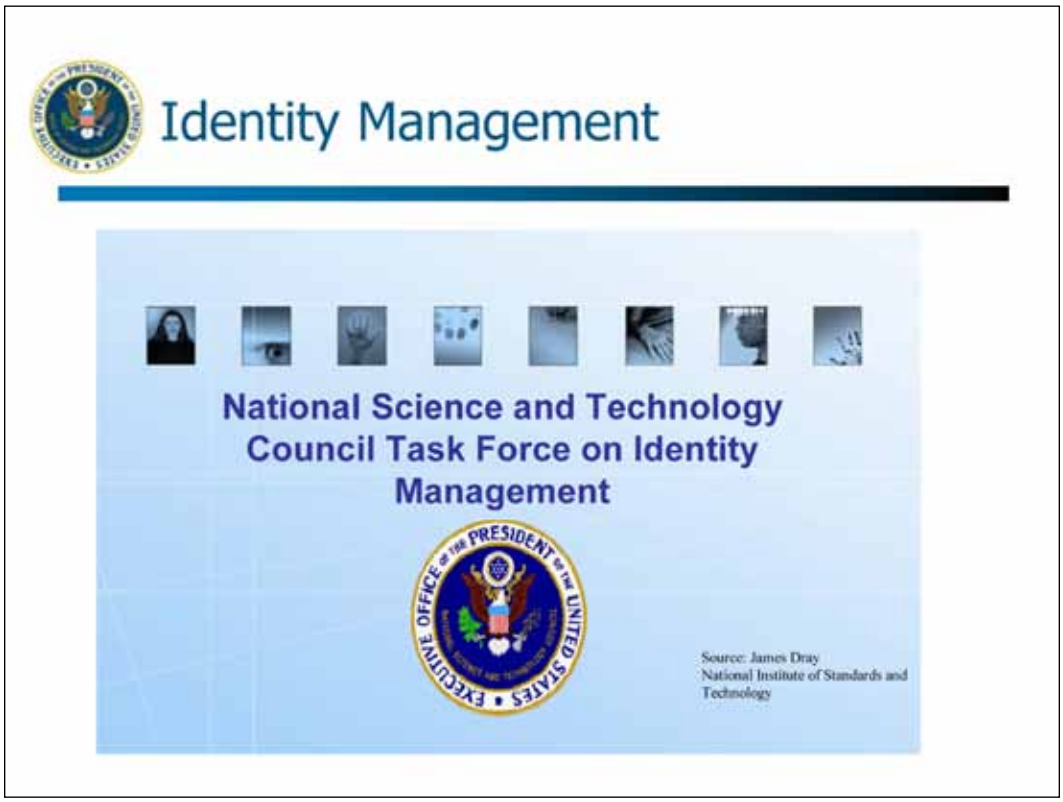

U.S. Networking and Information Technology R&D Investment
Investment ($M)
$4,000
$3,500
$3,000
$2,500
$2,000
$1,500
$1,000
$500
$0
1991
1993
1995
1997
1999
2001
2003
2005
2007
2009
'09 unclassified cyber security R&D is ~ $300M, up from ~ $190M in 2007

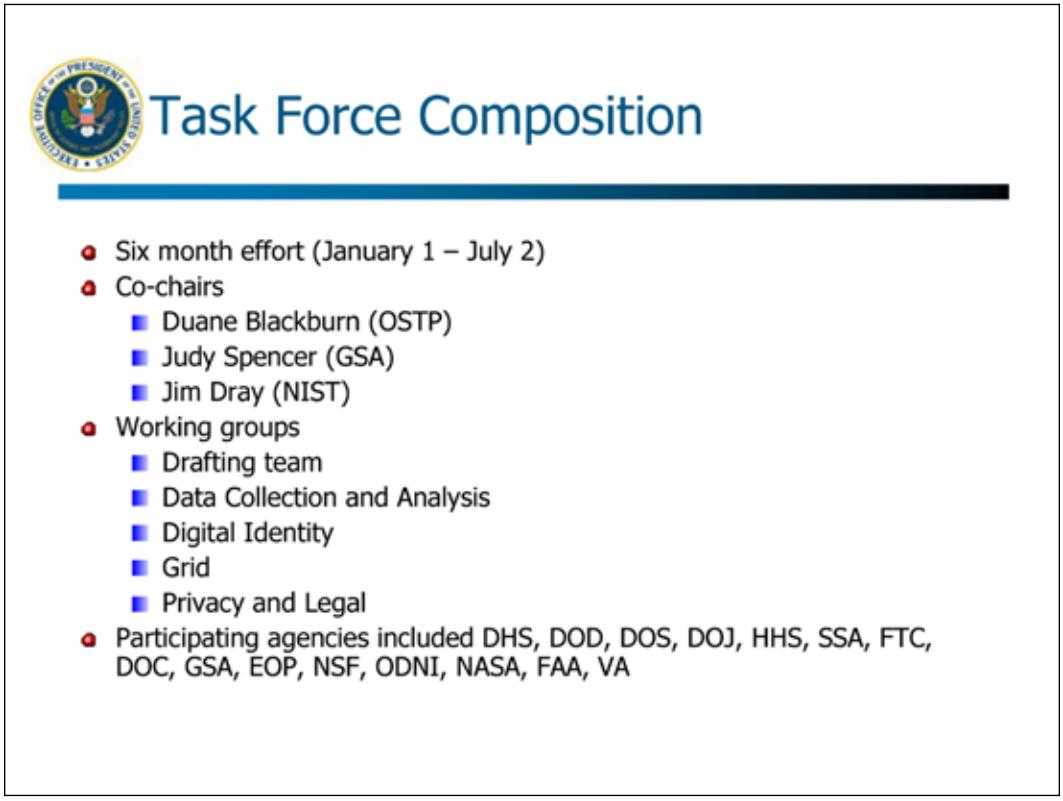

PCAST
EOP
OSTP
NSTC
Committee on Technology
NITRD Subcommittee
NCO
CSIA Senior Steering Group (CSIA SSG)
Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)
+
representative(s) of SCORE IWG
+
representatives of HCSS, LSN, and other NITRD PCAs as appropriate
SCORE IWG (classified R&D)
CSIA SSG members
• Agency NITRD co-chair
• Director, NCO
• Agency co-chair of SCORE IWG
• Senior representatives of agencies with national cyber security missions (e.g., DoD, DHS, NSA, NIST)
• OSTP, OMB ex officio

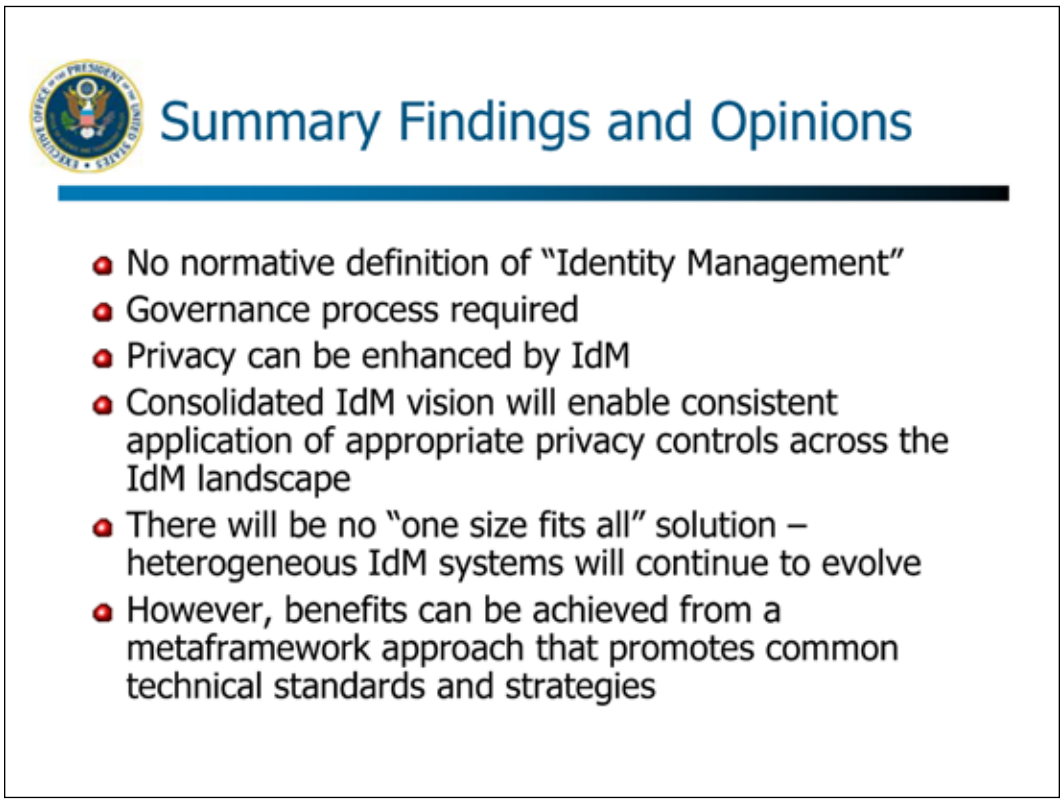

National Nanotechnology Initiative
Investment ($M)
1800
1600
1400
1200
1000
800
600
400
200
0
NNI launched
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009


International Nanotech R&D Investment
Investment ($M)
2500
2000
1500
1000
500
0
Asia
U.S.
Europe
Others
2000
2001
2002
2003
2004
2005
2006
2007
Lux Research public funding estimates as of 2007


APPLICATIONS – Energy Storage
High-Performance Batteries
20-30 nm particles aggregated into 1-5 μm particles
A123 SYSTEMS
m1
Terminal)
Gasket
Steel-Can (Negative Terminal)
Bottom Insulator
Anode Tab
Nanotechnology enables smaller, lighter, safer, and longer-lasting batteries that could meet the parameters for practical electric vehicles


Identity Management
National Science and Technology Council Task Force on Identity Management
Source: James Dray
National Institute of Standards and Technology


Task Force Composition
Six month effort (January 1 – July 2)
Co-chairs
Duane Blackburn (OSTP)
Judy Spencer (GSA)
Jim Dray (NIST)
Working groups
Drafting team
Data Collection and Analysis
Digital Identity
Grid
Privacy and Legal
Participating agencies included DHS, DOD, DOS, DOJ, HHS, SSA, FTC, DOC, GSA, EOP, NSF, ODNI, NASA, FAA, VA

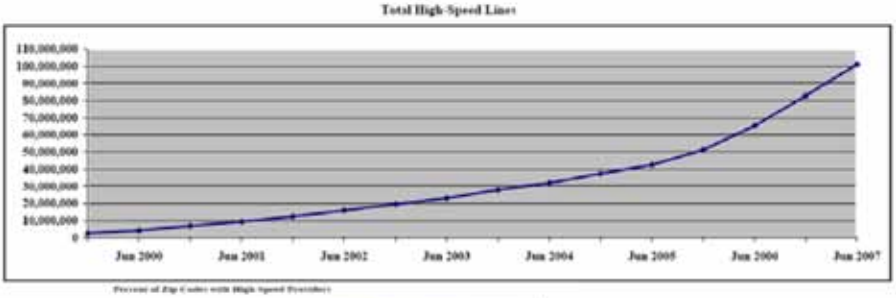

Summary Findings and Opinions
No normative definition of "Identity Management"
Governance process required
Privacy can be enhanced by IdM
Consolidated IdM vision will enable consistent application of appropriate privacy controls across the IdM landscape
There will be no "one size fits all" solution – heterogeneous IdM systems will continue to evolve
However, benefits can be achieved from a metaframework approach that promotes common technical standards and strategies

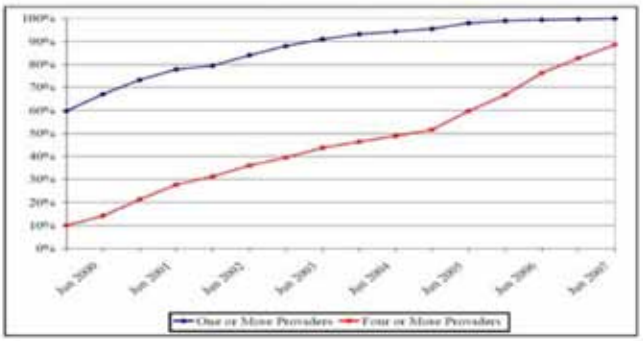
President Bush on Broadband

"We ought to have a universal, affordable access for broadband technology by the year 2007, and then we ought to make sure as soon as possible thereafter, consumers have got plenty of choices when it comes to purchasing the broadband carrier."

March 26, 2004

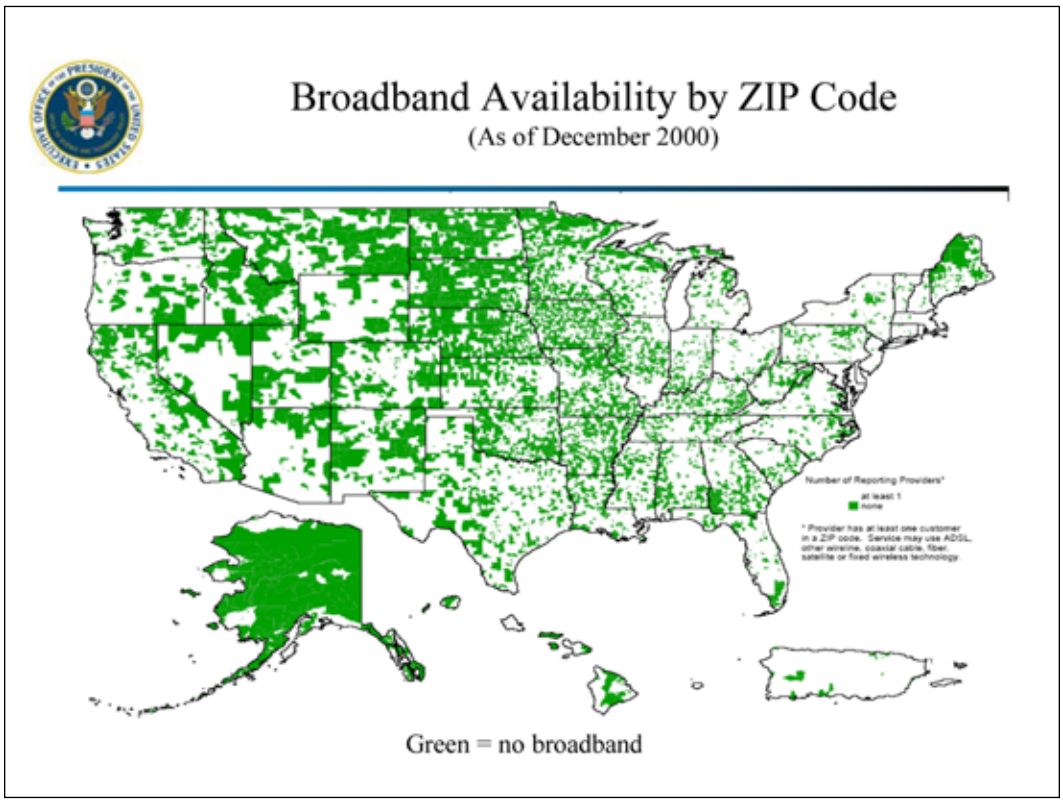
Broadband growth in US

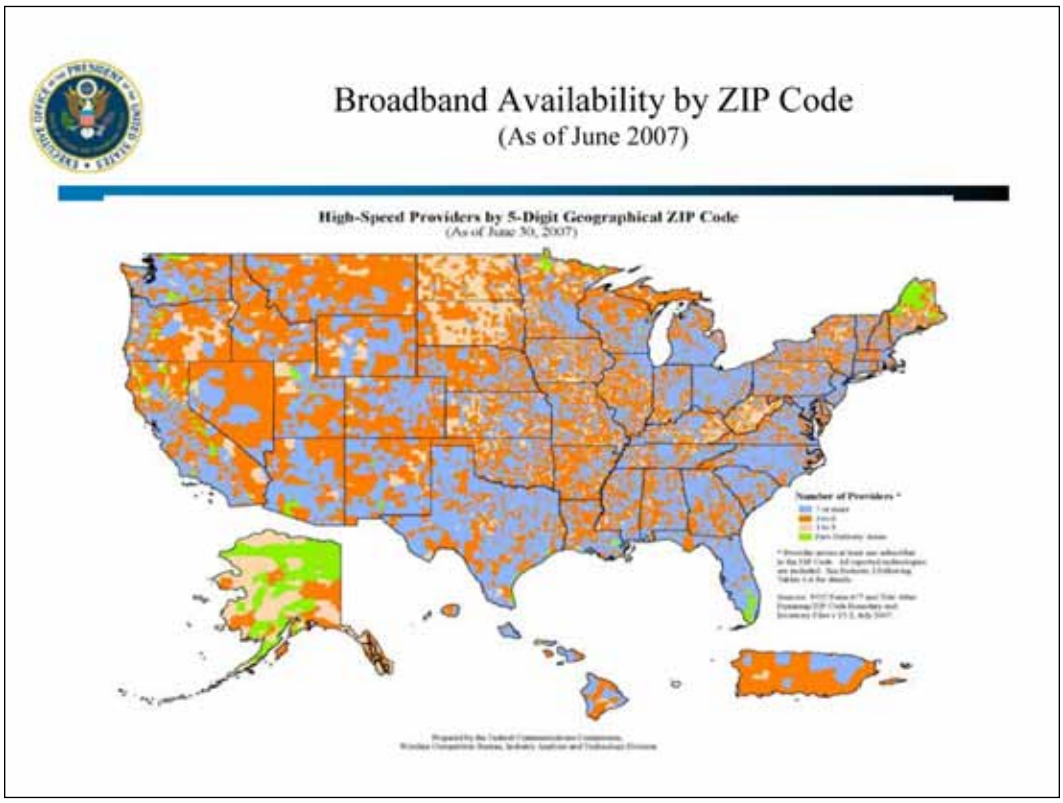




Broadband lines have increased from under 10 million at the start of 2001 to over 100 million lines in June 2007.

Source: FCC


Broadband Availability by ZIP Code
(As of December 2000)
Number of Reporting Providers*
at least 1
none
* Provider has at least one customer in a ZIP code. Service may use ADSL, other wireline, coaxial cable, fiber, satellite or fixed wireless technology.
Green = no broadband

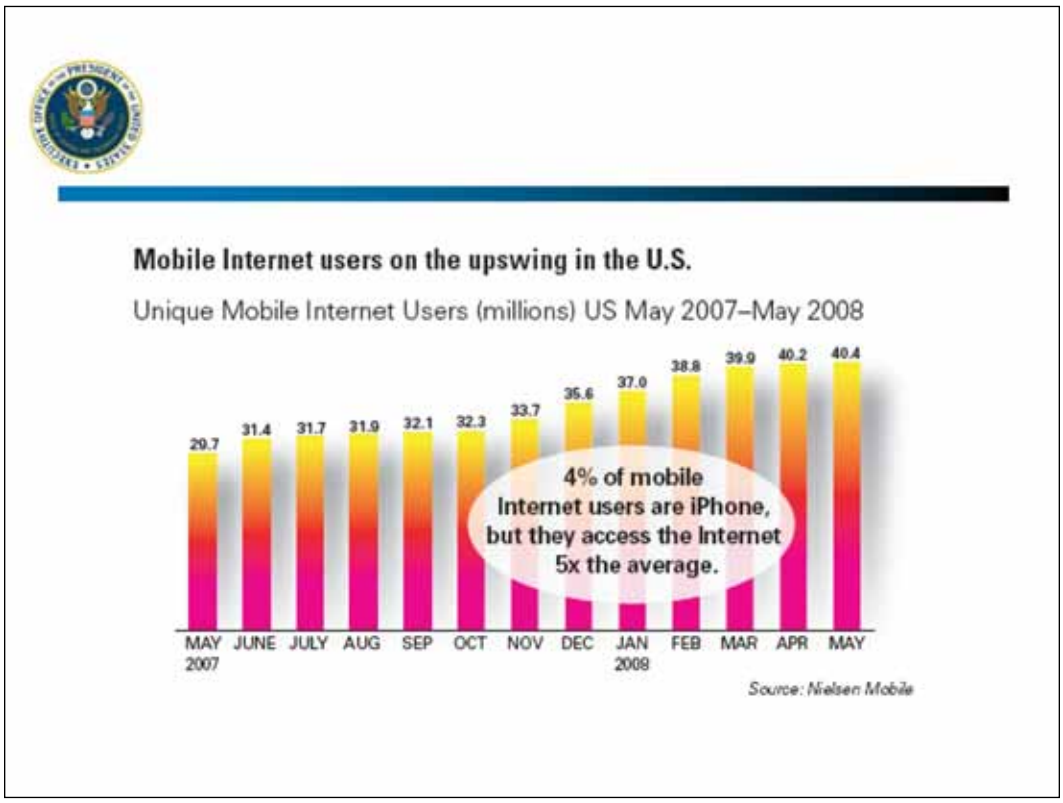

Broadband Availability by ZIP Code
(As of June 2007)
High-Speed Providers by 5-Digit Geographical ZIP Code
(As of June 30, 2007)
Number of Providers *

"The spectrum that allows for wireless technology is a limited resource… And we need to use it wisely. And a wise use of that spectrum is to help our economy grow, and help with the quality of life of our people… And so one of things we need to do is unlock the spectrum's value -- economic value and entrepreneurial potential without -- without, by the way, crowding out important government functions. And we can do both." -- President George W. Bush June 24, 2004

25

Spectrum Policy

WWW.DTV2009.GOV


Mobile Internet users on the upswing in the U.S.
Unique Mobile Internet Users (millions) US May 2007–May 2008
29.7
31.4
31.7
31.9
32.1
32.3
33.7
35.6
37.0
38.8
39.9
40.2
40.4
4% of mobile Internet users are iPhone, but they access the Internet 5x the average.
MAY 2007
JUNE
JULY
AUG
SEP
OCT
NOV
DEC
JAN 2008
FEB
MAR
APR
MAY
Source: Nielsen Mobile

Breakout Session Summary Slides

2008 RDX Workshop

Emergency Communications Breakout Session

Peggy Matson, Motorola
Dan Phythyon, Office of Emergency Communications

September 26, 2008

Emergency Communications: What ought to be…

Operability/Interoperability

- Appropriately secure interoperability across wireless networks with disparate protocols and frequency bands (i.e., private and public, legacy and next generation) without restricting mobility
- Ability to share media between government entities, to/from the general public (e.g. alerts, pictures), to/from operators of critical infrastructure
- Ready access to reliable communications for disaster response, including supplemental communications capabilities (e.g., satellite, rapidly deployable), communications that operate in starved environments (e.g., alternative energy), relocateable communications (e.g., Next Generation E911)
- Primary communications capabilities are built to withstand the physical punishment and heavy call load of a major disaster

Spectrum

- The ability to fully utilize whatever spectrum is best suited for the task, including the opportunistic use of secondary use spectrum (e.g. TV White Space) and unlicensed spectrum

Information Access and Exchange

- Access to and consolidation of volumes of all-media data to create easily consumable, user-tailored intelligence, and the presentation of such intelligence as to enable a highly informed yet without-delay incident response (e.g. high velocity human factors)

Current Enabling R&D Activities

- Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is currently coordinating a number of R&D activities, involving government, academia, and industry stakeholders
  - **Multi-band Radio (136-807 megahertz [MHz]) and Antenna**: Ability to communicate across multiple frequency bands using a single device
  - **Common Air Interface (CAI) and Inter Sub-system Interface**: Development of open architecture standards for interoperability
  - **Compliance Assessment Program (CAP)**: Establishing a testbed to validate TIA/EIA-102 Project 25 compliance of vendor products
  - **National Visualization and Analytics Center**: 6 regional university centers focused on developing algorithms to help interpret event information for decision making purposes
  - **Protection of Wireless Networks**: Working with ITS (Boulder, CO) to test the security of digital transmissions

Overarching Fundamentals

- The emergency response community should be involved in all R&D and policy initiatives, supported by industry and academia
- Funding is required to support proposed R&D and policy initiatives
- Technologies should be developed and deployed in a way that results in a graceful migration and leverages existing investments and resources (e.g., infrastructure, spectrum) to the greatest extent possible
- Interoperability requirement is not “everybody-to-everybody”

Technical Challenges and Initiatives: General

Challenge	R&D Initiative/Policy Implementation	Responsibility
Ability to justify R&D investment by industry based solely on public safety requirements	R&D: Aggregate strategic user requirements, including sustainability, across all levels of government (Federal, State, local, tribal) and defray risk/investment where there is no viable industry business case	Federal Government in coordination with Industry
Transfer of technologies in use within the Department of Defense into affordable commercial products for emergency response agencies	Policy: Identify DoD technologies that can be integrated/adapted cost effectively by civil government agencies. Strengthen and fund the 1401 and 1033 programs R&D: Adapt DoD technologies for public safety use	Federal Government in coordination with industry Industry
Limited solutions/approaches for system lifecycle planning	Policy: Support Federal technical assistance programs to assist emergency response agencies with system lifecycle planning that includes solutions/approaches for technology migration and sustainment	Congress through the Executive Branch

Technical Challenges and Initiatives: Operability/Interoperability (1 of 3)

Challenge	R&D Initiative/Policy Implementation	Responsibility
Ability for users to roam across systems	R&D: Develop a universal handheld device that enables mobility and roaming across systems, including affordability, authentication (user and device), and multi-band antennas Policy: Develop a policy architecture and technology to help execute policy	Industry in coordination with Government Federal Government
Lack of understanding of the security impacts (e.g., privacy) of existing and new technologies (e.g., cognitive radio) in an emergency response environment	R&D: Establish security testbeds (laboratory and pilots) for the automated evaluation of vulnerability of existing and new technologies in a public safety environment Policy: Determine the impacts of new technologies on privacy and the impact of privacy rules on the application of potentially essential technologies	Federal Government through Industry Federal Government through Industry
Availability associated with public safety/national security priority and preemption in the new mobility model	R&D: Determine the availability and priority services and enabling technologies (e.g., end-to-end, QoS, audio quality, authentication) in the new mobility model Policy: Determine the process and policy impacts of preemption in the new mobility model	Federal Government through Industry Federal Government

Technical Challenges and Initiatives: Operability/Interoperability (2 of 3)

Challenge	R&D Initiative/Policy Implementation	Responsibility
Disparate security techniques across agencies	Policy: Determine a security framework for national use by public safety (e.g., national PKI)	Federal Government in coordination with industry
Ability to regenerate power and reduce consumption for communications capabilities when strained	R&D: Research and develop alternate power sources (e.g., fuel cells) to temporarily provide power and reduce power consumption when communications capabilities are strained	Federal Government through Industry
Lack of common standards for data exchange	R&D: Continue to support the standards development process with focus on data format and data exchange protocols	Continued participation from Government and Industry
	R&D: Development of technologies (e.g., social networking) to support co-decision making and data sharing across emergency response coordination points across levels of government	Federal Government in coordination with Industry
	Policy: Develop common lexicons for plain language	Federal Government

Technical Challenges and Initiatives: Operability/Interoperability (3 of 3)

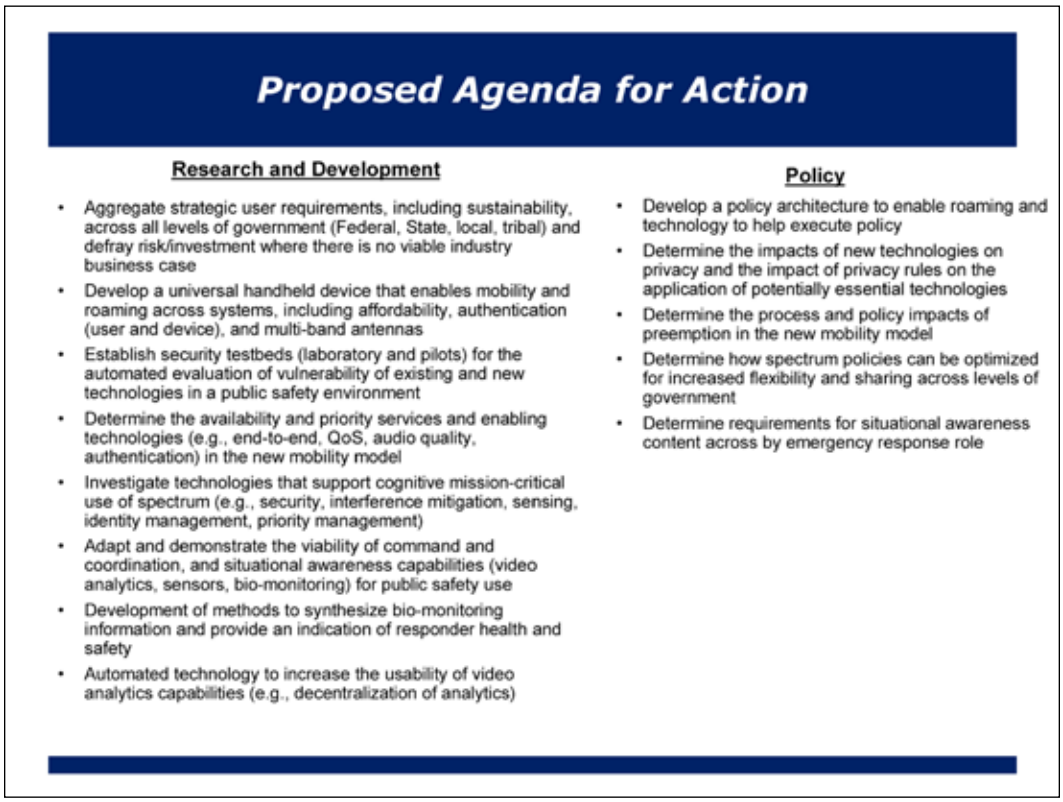
Challenge	R&D Initiative/Policy Implementation	Responsibility
Capability to aggregate, authenticate, prioritize, and distribute alerts and warnings, and them across networks	R&D: Develop the capability to aggregate, authenticate, prioritize, and distribute public alerts and warnings	Federal Government through Industry
	R&D: Determine method for geographically distributing public alerts and warnings	Federal Government
	Policy: Establish roles and responsibilities for the aggregation, prioritization, and delivery of public alerts and warnings	Federal Government
Lack of a business case for satellite service providers to offer immediately available capacity for emergency response agencies	Policy: Study the ability to establish a business case for immediately available capacity for emergency response agencies	Federal Government through Industry
Deployment of new technologies without adequate testing and evaluation (e.g., vocoder)	R&D: Establish a framework for development and evaluation of new technologies in a multidisciplinary public safety environment	Federal Government through Industry

Technical Challenges and Initiatives: Spectrum

Challenge	R&D Initiative/Policy Implementation	Responsibility
Ability to optimize spectrum use in support of the emergency communications mission	R&D: Investigate technologies that support cognitive mission-critical use of spectrum (e.g., security, interference mitigation, sensing, identity management, priority management)	Federal Government through Industry
	Policy: Determine how spectrum policies can be optimized for increased flexibility and sharing across levels of government	Federal Government
Lack of understanding of how broadband will be used to support emergency response	Policy: Investigate the use of broadband to support emergency response	Federal Government

Technical Challenges and Initiatives: Information Access and Exchange

Challenge	R&D Initiative/Policy Implementation	Responsibility
Need for improved command and coordination, and situational awareness capabilities to support emergency response missions	R&D: Adapt and demonstrate the viability of command and coordination, and situational awareness capabilities (video analytics, sensors, bio-monitoring) for public safety use	Federal Government through Industry
	R&D: Development of methods to synthesize bio-monitoring information and provide an indication of responder health and safety	Federal Government through Industry
	R&D: Automated technology to increase the usability of video analytics capabilities (e.g., decentralization of analytics)	Federal Government through Industry
	Policy: Determine requirements for situational awareness content across by emergency response role	Federal Government


Proposed Agenda for Action
Research and Development
Aggregate strategic user requirements, including sustainability, across all levels of government (Federal, State, local, tribal) and defray risk/investment where there is no viable industry business case
Develop a universal handheld device that enables mobility and roaming across systems, including affordability, authentication (user and device), and multi-band antennas
Establish security testbeds (laboratory and pilots) for the automated evaluation of vulnerability of existing and new technologies in a public safety environment
Determine the availability and priority services and enabling technologies (e.g., end-to-end, QoS, audio quality, authentication) in the new mobility model
Investigate technologies that support cognitive mission-critical use of spectrum (e.g., security, interference mitigation, sensing, identity management, priority management)
Adapt and demonstrate the viability of command and coordination, and situational awareness capabilities (video analytics, sensors, bio-monitoring) for public safety use
Development of methods to synthesize bio-monitoring information and provide an indication of responder health and safety
Automated technology to increase the usability of video analytics capabilities (e.g., decentralization of analytics)
Policy
Develop a policy architecture to enable roaming and technology to help execute policy
Determine the impacts of new technologies on privacy and the impact of privacy rules on the application of potentially essential technologies
Determine the process and policy impacts of preemption in the new mobility model
Determine how spectrum policies can be optimized for increased flexibility and sharing across levels of government
Determine requirements for situational awareness content across by emergency response role

2008 RDX Workshop

Convergent Technologies Breakout Session

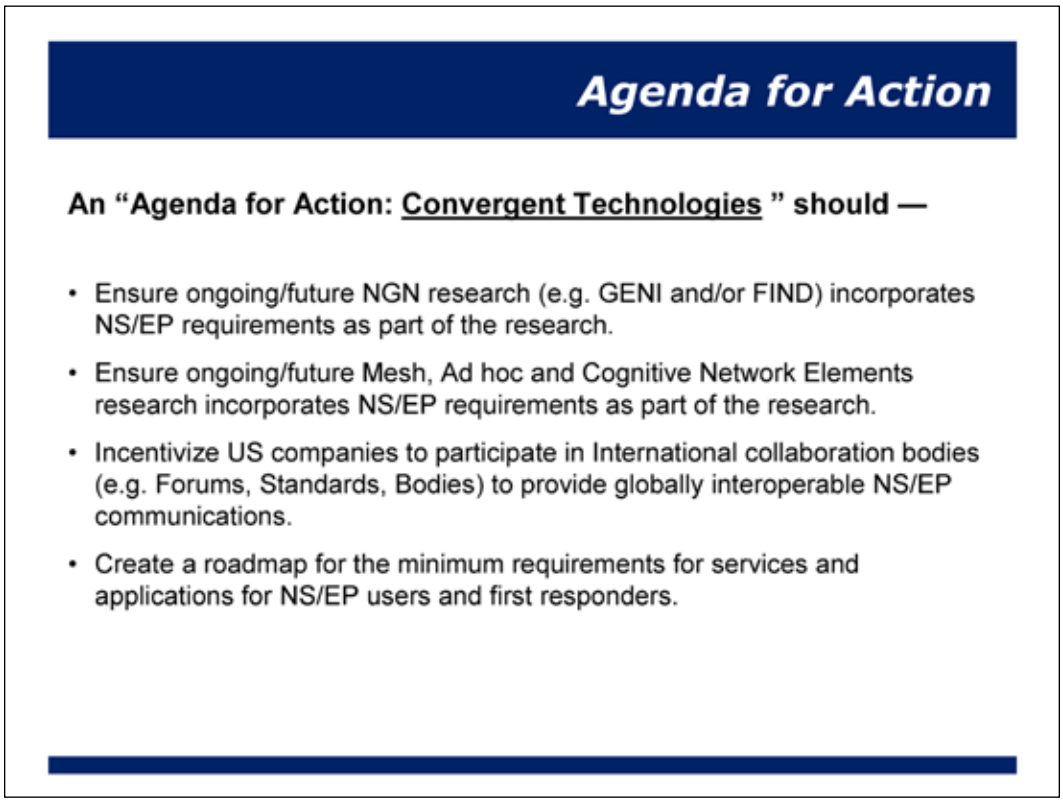
Patrick Beggs, DHS
Patrick.Beggs@dhs.gov
Jim Mathis, Motorola
Jim.Mathis@motorola.com

September 25-26, 2008

Challenges & Priorities

Members of the Convergent Technologies breakout session identified the following critical challenges and new priorities for further R&D:

- NS/EP requirements factored into US and International research.
- Prioritization, Interoperability and Security capabilities are needed above the transport Level:
  - Dynamic situational awareness and the ability to adjust accordingly to the technology needs.
  - Mission based situational framework.
- Ability to reconstitute operations and critical infrastructure in the event of a catastrophic event (e.g.):
  - Alternate power/limited power.
  - Alternate delivery/communications channels.


Agenda for Action
An "Agenda for Action: Convergent Technologies " should —
• Ensure ongoing/future NGN research (e.g. GENI and/or FIND) incorporates NS/EP requirements as part of the research.
• Ensure ongoing/future Mesh, Ad hoc and Cognitive Network Elements research incorporates NS/EP requirements as part of the research.
• Incentivize US companies to participate in International collaboration bodies (e.g. Forums, Standards, Bodies) to provide globally interoperable NS/EP communications.
• Create a roadmap for the minimum requirements for services and applications for NS/EP users and first responders.


Agenda for Action
An "Agenda for Action: Convergent Technologies " should —
• Identify policy framework and related research as they pertain to prioritization for both transport and applications (i.e. web / hosted application, cloud computing framework, SaaS, Carrier traffic management).
• Further development of modeling and simulation, forensics, and trusted relationships constructs during NS/EP events (i.e. multiple peering point destruction, cyber attacks, DDoS, overall traffic saturation).
• Initiate research to develop and deploy network elements that allow for quicker reconstitution using alternative/limited power sources in the event of a national emergency.

Backup

Current R&D Activities

The following R&D activities are currently underway which address Convergent Technologies and serve to strengthen NS/EP communications:

- IETF working groups, e.g., Pre-congestion Notification (pcn)
- Internet Research Task Force, e.g., Internet Congestion Control (iccrg) & IP Mobility Optimizations (mobopts)
- Next Generation Internet Internet2 Qbone Premium Service (QPS)
- GÉANT & GÉANT2 projects
- DNSSEC, BGP security, DETER testbed
- GENI and FIND next generation projects
- DSN (Defense Switched Network) Assured Services Research
- NCS Modeling and Simulation Research

Key Technology Areas

Specific technology areas offer the most potential to improve Convergent Technologies R&D in the future:

*(Use an * to indicate which technology areas should receive the most attention)*

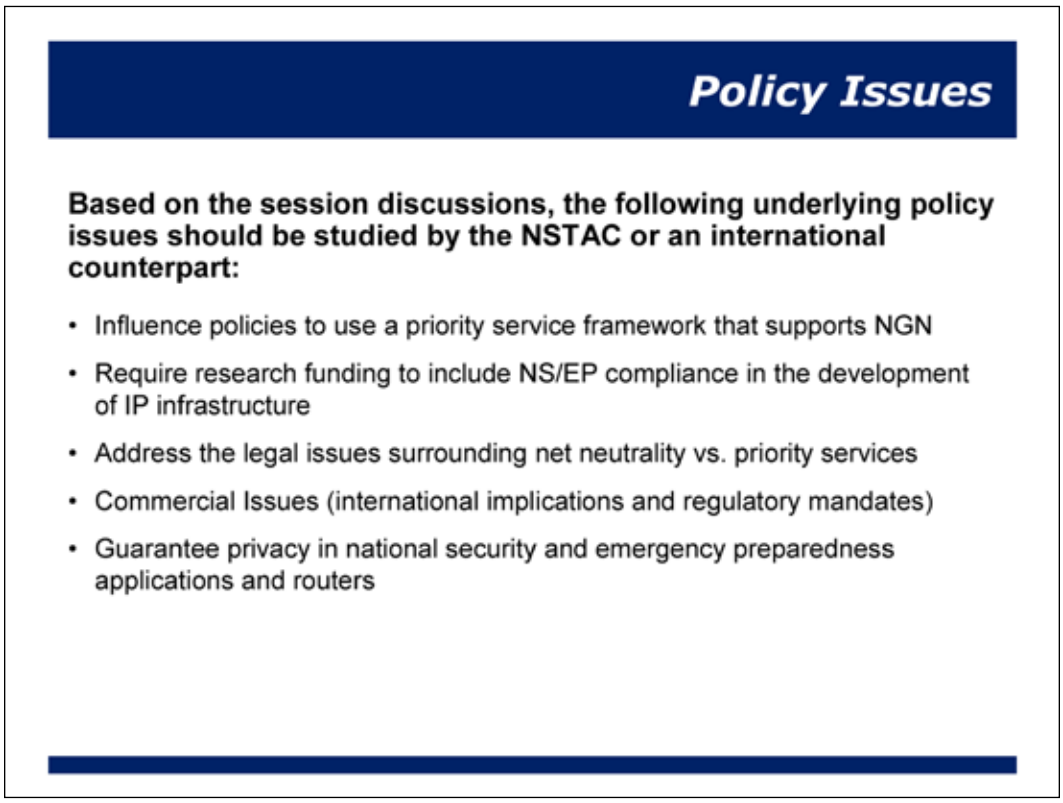
- Mitigation of degraded network environment
- Prioritization of Applications and Services*
- Development of Mesh Ad hoc / Cognitive Network Elements
- Addressing the limitations of Internet Protocol (IP)
- Creating authentication and priority at Layer 1 or Layer 2
- Configuring or developing network elements that pull less power
- Creation of Forensics or "CSI" tools in a converged network environment to analyze network attacks

**** These areas are the highest priority areas and should receive immediate attention.***

Potential Impediments

Impediments that might inhibit solution deployment to advance Convergent Technologies in the future are:

- Pervasiveness of the legacy IPv4 protocol
- Not all traffic traverses United States networks
- Limitations of IPv6 to maintain and recognize packet header information
- Adoption of an effective protocol
- Driving the business case for key stakeholders
- Net Neutrality Legislation
- Lack of a mechanism to determine international / local/ national agreement


Policy Issues
Based on the session discussions, the following underlying policy issues should be studied by the NSTAC or an international counterpart:
• Influence policies to use a priority service framework that supports NGN
• Require research funding to include NS/EP compliance in the development of IP infrastructure
• Address the legal issues surrounding net neutrality vs. priority services
• Commercial Issues (international implications and regulatory mandates)
• Guarantee privacy in national security and emergency preparedness applications and routers

2008 RDX Workshop

Defending Cyberspace Breakout Session

Mr. Robert Dix, Juniper Networks
Mr. Robert Leafloor, Industry Canada

September 26, 2008

Agenda

- General Cyber Defense Issues
- Current R&D Environment
- Potential Impediments
- Possible Incentives
- Top Four Issues and Recommendations

General Cyber Defense Issues

- Risk Management
  - Need for realistic *threat* data for industry to input into risk calculations
  - Debate concerning the definition and importance of *vulnerabilities*
  - Need for risk assessments to be conducted to identify gaps which can then drive prioritization of R&D efforts
- Issue of accountability and responsibility
- Idea of a national cyber boundary (defense-in-depth)
- Mission assurance translates into resilience
- Need to develop a strategy around deterrence and attribution
- Lack of strong business case to drive industry to action
- Cyber defense has been pushed to the end user who is generally ill-equipped to address, or ignorant of, the security solutions -> "grandma" factor
- Issue of integrity as it relates to the supply chain process
- Lack of awareness on part of consumer and industry

Current R&D Environment

- General questions
  - Where are we today?
  - Where do we need to be in the future?
- Collective sense that there is a lot of room for improvement in government and industry collaboration on cyber defense R&D efforts
- Lacks metrics to measure the value of previous R&D investments
- Lack of a government inventory or database of past and current R&D efforts available to all stakeholders
- Lack of implementation of tools and technologies that result from current R&D efforts
- Faces the on-going issue challenge of classification of R&D efforts

Potential Impediments

Impediments that inhibit collaborative R&D efforts in advancing future cyber defense:

- Privacy issues
- Globalization
- Budgets
- Human capital – shortage of graduates in CS/engineering as well as lack of forward-thinking curriculum
- Traditional or closed thinking in a dynamic environment
- Classified nature of many R&D efforts

Possible Incentives

Incentives that might help drive collaborative R&D to advance cyber defense in the future are:

- Expand existing scholarship programs to encourage college students to pursue careers in cyber security and create partnerships between government and industry to offer students position in industry
- Increase incentives to commercial firms that keep R&D efforts on shore or bring them back on shore
- Use patents which will allow companies that develop new technologies to be sole provider for a given period of time
- Streamline the process of getting new technologies into the market to defend cyberspace

Four Issues

- What are four issues that would impact industry and government collaboration in area of R&D in the fight to defend cyber space?
- What are recommendations to achieve that?

Issue #1

- **R&D is needed to develop a bi-directional architecture and system of processes to establish a National Cyberspace Defense System.**
  - This system would defend infrastructure in the US from attacks so that every node on our networks is not left to defend itself. The system would necessarily operate as a collaborative program with industry and leverage information about known threats gathered from across industries and government.
  - Such a system would diminish the impact of attacks from our enemies, raise the cost of the attacks for our enemies, and accelerate recovery from attacks by enabling containment. Grandma would not be left to defend herself from attack, foreign and domestic.

Issue #2

- **R&D for Behavioral Science as it relates to development and propagation of malicious code and activities in order to be more predictive:**
  - Profiling of hackers, hacker groups and communities
  - Identifying the source and path or life cycle of malware systems based on how it morphs, grows and spreads or dies over time and the internet
  - Modeling correlations between release of information (software, magazine article, press release etc.) What triggers a person to write malware, and what are their behaviors throughout the process from idea through design, testing, implementation and upgrade?
  - Modeling of how a hacker, hacker group or community develops target selection and development. Motivations, incentives, risk analysis that drive and affect their decision to act or not.

Issue #3

- **Results of R&D efforts are not widely implemented:**
  - There is a need to investigate why this is the case and to look at how a range of incentives, or the removal of disincentives, could contribute to addressing this fundamental problem.
  - Identified the need to ascertain the progress of current cyber defense R&D efforts – what have all the previous R&D investments bought us? (goes back to 2003 RDX recommendation)
  - Identified the need for a government inventory or database of past and current R&D efforts to be available for all stakeholders
  - Ensure that security succeeding generations network is built secure from the ground up in a collaborative

Issue #4

- **Need for R&D efforts toward establishing the value in licensing as a tool to establish a security baseline.**
  - Conduct research to develop a licensing process for US based ISPs that would require the US ISPs to adopt and maintain cyber security practices commensurate with the most relevant risks as communicated by the government (agency to be determined). For foreign providers, the government will inform the US customers of the risks associated with the foreign option.

2008 RDX Workshop

Identity Management (IdM) Breakout Session

Facilitator Report

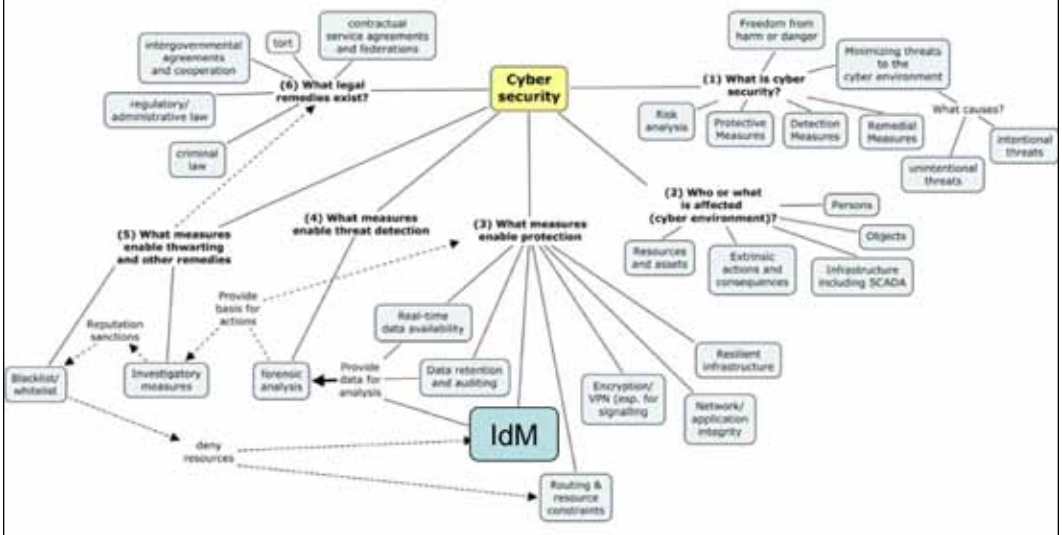
September 26, 2008

IdM Breakout Session Team

- Our Facilitators:
  - Mr. James Zok, CSC, jzok@csc.com
  - Mr. Tony Rutkowski, VeriSign, trutkowski@verisign.com
- Our Team:
  - 10 participants (ideal size for open dialog)
  - Public- and private-sector representation (Government, providers, vendors)
  - Deep IdM subject matter expertise:
    - R&D (e.g., biometrics, trusted computing)
    - Standards development (e.g., ITU, ISO)
    - Policy development (HSPD-12, US-VISIT)
    - IdM solutions implementation

IdM Breakout Session Team

IdM in Cyber Security Context



Standards/R&D Activities

Numerous and disparate IdM standards and related activities are underway which can serve to strengthen NS/EP communications (with better collaboration):

- ITU (e.g., X.1250: *Capabilities for Enhanced Global IdM Trust and Interoperability, Y.2720 IdM Framework for NGN*)
- DOD initiatives
- NSTC IdM Task Force Report
- NGN
- SCADA
- ISO (e.g., SC27 and 37)
- ANSI (e.g., M1)
- NIST/FIPS 201
- Liberty Alliance
- OASIS
- OpenID
- CardSpace
- Higgins
- Shibboleth
- NSTAC RDTF
- Many others…

IdM Activities – A Coordination Conundrum

- A US Federal Government perspective (one of many):

"List and describe the IdM collaborative efforts your organization participates in."
- NSTC Task Force Inventory of Federal IdM Systems

DOD Biometrics Task Force (BTF)
Attribute Based Access Control Working Group (ABACWG)
Biometrics Security Consortium
Biometrics Coordination Group
Committee on National Security Systems
Cyber Security Sub Council
DMDC Working groups
Defense Enrollment Eligibility Reporting System
Defense Science Board Task Force on Defense Biometrics
DOD IPMSCG
DOD PKI Certificate Policy Management WG
E-Authentication E-Gov initiative
Evaluation Program Technical WG
Federal Identity Credential Committee (FICC)
Federal PKI Policy Authority
ODNI Federated ID management pilot
FISMA initiative
Government Smart Card Interagency Advisory Board
GSA E-Authentication Technical WG
GSA HSPD-12 architecture working group (AWG)
GSA PKI Working Group
HSPD-12
ISC (Interagency Security Committee)
ISO/IEC SC 37 (Biometrics)
ISO/IEC/JTC1/SC27 (IT Security Techniques)
NCITS M1 (Biometrics)
NSTC Subcommittee on Biometrics and IdM
OASIS
Security Industry Alliance (SIA)
SmartCard Alliance (SCA)
SmartCard IAB (Industry Advisory Board)
SSN Tiger Team
Treasury Privacy Committee

- **Need for more coordination and alignment of existing activities**
- **Need for better exchange of information, results, and event horizons**

Key Technology Areas

- Biometrics
  - Infrastructure
  - Increase performance by x%
- Technologies for establishing interoperability and trust
  - Common credentials
  - Not just end user IdM, also provider and identity provider IdM
  - Ease of use
- Federated identity
- Discovery of authoritative identity information on global-scale
- New scalable/extendible architectures (e.g., SOA)
- Others:
  - PKI/PKI Infrastructure (implementation)
  - "Multimode" cards (integration of multiple solutions)
  - IdM of objects and object binding (e.g., location awareness)

Key Challenges in IdM Space

TRUST

- Vetting (trusting credential issuer, 3rd party, original source)
- Need for audit regime (e.g., extended validation certificates on web)
- Reciprocal trust methods to verify agreements
- Tying individual identity to device/device to provider
- What is trust model? (e.g., size, scale)
- Root ID issue (e.g., passport)
- Anonymity (as opposed to privacy-owner consent)
- Authentication

POLICY

- Business processes/Business models
- Need for business case to support pervasive use
- International acceptance (e.g., via federated identities, standards bodies) – who should be responsible?
- Scope is both national and international. (authority and jurisdictional issues)
- Promoting US interests in standards bodies

Key Challenges in IdM Space

TECHNOLOGY

- Usability/Ease of Use
  - Drive adoption/pervasiveness
  - Cultural, business, technical, policy components at play
  - "Shooting for the moon" at the expense of wider user acceptance
- Context Dependency
- Biometrics (e.g., accuracy, cost, future advances [cognitive brain wave, DNA])
- Better forensics to verify ID
- How do we deal with differences in pace of progress?

SOCIAL ISSUES

- Privacy (several definitions)
- Cultural differences
- Socialization of Control of Identity
- Usability/Ease of Use
  - Generational "technology acceptance

IdM Priorities for R&D

- Interoperable trust mechanism
  - Certification & Accreditation; Auditing
  - Standardization of Strength of Authentication
  - Lessons Learned from other models (e.g., Space, health care)
- Vetting processes
- IdM-specific Infrastructure
  - Security of data and its transmission
- Biometrics beyond performance (e.g., end-to-end solutions)
- Non-user-based IdM:
  - Binding "non-user" identities (e.g., objects, devices, applications)
  - Coupling of Technologies
  - Other Technologies for Identification (e.g., RFID)
- Discovery (sources of authoritative identity information)

Policy Issues - NSTAC study candidates

- Need for new organizational approaches/entity with proper authority and jurisdiction
  - Herding Cats Problem
  - How to Facilitate Focus/Coordination/Cross Fertilization
  - Need for IdM Czar?
  - Roles and Partnerships (who owns the problems)
  - Federation processes
  - Enhanced international collaboration
  - Review existing policies
  - Review Policy Enforcement (e.g., CAC card acceptance/use)
  - Identify incentives for IdM implementation (e.g., PPP, grants, business cases, tax-based)
- Incentives for academic participation in IdM Standards bodies (e.g., other nations):
- Privacy/PII
- Role of Regulation
- Allocation of Funding/Effective processes for funding organizations (e.g., NSA, NIST)

A "Game-Changing" Agenda for IdM Action

Most if not all public infrastructure IdM capabilities are inherently NS/EP related.

- Publish an NSPD to create an IdM Coordination Office which will:
  - Provide oversight
  - Identify roles/responsibilities in the area (e.g., delineating inherently governmental vs private-sector IdM functions)
  - Drive interoperable infrastructure development
  - Identify and establish incentives to drive IdM business cases/private sector adoption
- Issue an OMB policy guidance directive for the next fiscal year which incentivizes synergistic participation in standards bodies as a stipulation for IdM R&D funding
- Direct NSA to establish the rules/processes for implementing IdM solutions (at all levels including privacy protection)
  - Establish effective, common, global, IdM infrastructure and supporting mechanism(s) for service providers

2008 RDX Workshop

Emerging Technologies Breakout Session

Siafa Sherman, Nortel

September 25-26, 2008

Key Technologies

Trusted Architecture – A model that enables secure reliable end-to-end communications, structure, and data in the NS/EP environment

- **Problem Statement:**
  - **No end-to-end integration solution to provide a trusted environment for application and data access**
- **Challenges/Gaps:**
  - **Most solutions are proprietary**
  - **Current inability to align industry to provide a complete standard solution**
  - **Align industry, academia, and Government**
- **Solution:**
  - **Research required to develop a security model that addresses:**
    - **Standards and integration**
    - **End devices including silicon based implementations**
    - **Communications and data transport**
    - **Identity management and access controls**
    - **Data self protection**
    - **Application and software coding standards for security**
    - **Integration of security into systems development life-cycle (SDLC) through training, education, and mandatory certification for critical applications development**

Key Technologies

Trusted Architecture (continued)

- **Impact Statement:**
  - **Enables secure cloud and peer computing**
  - **Strengthens security posture overall**
  - **Implements a standard security model with similar benefits to the OSI model**
  - **Defines the security attributes across all layers**

Key Technologies

Distributed/Portable Energy Technologies (Battery, Fuel Cells, Solar Cells, Kinetic Chargers) – Essential for the success for NS/EP long term strategies and operations

- **Problem Statement:**
  - The energy demand for infrastructure is exponentially growing;
  - The network has become integral to NS/EP and social survival;
  - NS/EP Infrastructure disruptions due to energy loss equates to social breakdown.
- **Challenges/Gaps:**
  - **Energy Generation**
    - Individual energy generation solutions must be hybridized (e.g. battery + solar + kinetic + fuel = energy supply for network)
    - TELCO sector Independent energy generation
    - New innovative solutions for power generations from **miliwatt to watt** to megawatt
  - **Energy/Power Management**
    - Intelligent COOP
    - Source Management of distributed hybrid solution
    - On-demand distribution and prioritization
  - **Energy Usage**
    - Increased efficiency of infrastructure components
    - Software based energy controls
    - Energy smart infrastructure devices

Key Technologies

Distributed/Portable Energy Technologies (Battery, Fuel Cells, Solar Cells, Kinetic Chargers) - Continued

- **Solution:**
  - Self sufficient local energy generation nodes
  - Hybrid, solar, wind, battery, other
  - 10X chip power use reduction
  - 10X battery capacity
  - Room temperature super conducting wire
  - 10X increase in power management
  - New materials research for energy
- **Impact Statement:**
  - Negative
    - Social survival- food, money, energy and water flows are all dependent upon the network
  - Positive
    - Rapid recover of infrastructure in the face of crisis event
    - Sustained infrastructure during a extended crisis
    - Fast infrastructure recovery increase recovery of all social needs

Key Technologies

Assured Attribution

- **Problem Statement:**
  - Today it is difficult or impossible to assure the attribution of the source of bad actions that disrupt service, fraud, terrorist activity etc. or nation-state attacks in cyber space
- **Challenges/Gaps:**
  - Global Support
  - Privacy Issues
  - Immature techniques that support heuristics for accurate data collection
  - Inefficient data mining and visualization due to lack of sufficient attribution
- **Solution**
  - We need a research effort that would focus on how to enhance attribution techniques, to include the above suggested
  - Need a consortium effort among government, industry and academia to focus on the development of such techniques and address privacy issues

Key Technologies

Assured Attribution (continued)

- **Impact Statement:**
  - More accurate and rapid attribution capability
  - May serve as a deterrent to some actors

Key Technologies

Dynamic Spectrum Access – DSA is a new technology that promotes efficient and flexible use of spectrum by sensing spectrum availability and assigning the use in real time. This capability enables integration of wireless and fixed network infrastructure that contains intelligent systems that control the spectrum assignments

- **Problem Statement:**
  - Demand for spectrum is increasing, spectrum is a finite resource, becoming increasingly scarce; current static spectrum management approach exacerbates the problem by dedicating frequencies to stovepipe wireless systems
- **Challenges/Gaps:**
  - Challenge - To develop a dynamic spectrum reuse approach that enables effective and efficient use of limited spectrum resources
  - Gap - Requires a paradigm shift in spectrum management (i.e., processes, regulatory, policy) and spectrum access technologies
- **Solution:**
  - R&D: substantial R&D funding is needed to bring DSA to maturity; sponsorship from senior leaders; involve the integration of existing architecture and will require a migration strategy and has policy, technology and regulatory implications.
- **Impact Statement:**
  - Increases spectrum availability to accommodate new uses; expands network capabilities by providing mobile access to content and functionality that currently resides in fixed networks; as a whole, improves utilization resources (i.e., spectrum, network resources)

Other Technologies

Other Technologies Considered:

- **Social Network Technologies**
  - **Web 2.0/SOA**
- **Integrated Federal Enterprise Backbone** (a game changer)
- **Converged IP Technologies**
- **Cloud Computing** – Allocating trust into the cloud (can't always restrict rights to data in Cloud Computing). Platform needs to have capability to feed in verifiers – identity attributes in device, application, and data

Other NS/EP Problems to Solve

Other NS/EP Problems Discussed to Solve Through Technologies:

- What if the Internet breaks? Back-up architecture/structure
- Need for reliable infrastructure
  - (risk with cloud computing of technology being taken down)
- High-speed and personalized data transfer capability (essential for cloud computing)
- Location based sensors
  - Indoor (inside building) location tracking/situational awareness
  - National Security concerns with being located by malicious actors (e.g., police location, etc.)
  - Beneficial for emergency responders
- Prioritization of network traffic (from operators stand point)
  - Based on who players are
  - Data prioritization

Current R&D Activities

The following R&D activities are currently underway, which address challenges presented by emerging technologies and serve to strengthen national security and emergency preparedness communications:

- Security on the Chip (Intel)
- Wireless Sensor Networks
- Distributed Energy Technologies (globally)
  - DARPA and others
- Cognitive Radio/SDR (DARPA, Motorola, Nortel)
- Converged IP Architecture Vulnerabilities
- Engagement with Standards Setting Groups
  - DOD engagement with industry (through IEEE Meetings)

Potential Impediments

Impediments that might inhibit collaborative R&D to advance technologies in the future are:

- Budgetary Constraints
- Lack of Executive Level Sponsorship
- Intergovernmental Governance and Policy Enforcement

Challenges & Priorities

Members of the emerging technologies breakout session identified the following critical challenges and new priorities for further R&D:

- **Trusted Architecture**
  - Most solutions are proprietary
  - Current inability to align industry to provide a complete standard solution
  - Align industry, academia, and Government
- **Distributed/Portable Energy Technology**
  - Energy Generation
  - Energy/Power Management
  - Energy Usage
- **Assured Attribution**
  - Broad global support for the following efforts would be required
  - Privacy Issues
  - Techniques that would support heuristics to enable the accurate collection of information that would enhance the efficiency of data mining and visualization to accomplish attribution need to be significantly improved
- **Dynamic Spectrum Access**
  - Development of a dynamic spectrum reuse approach that enables effective and efficient use of limited spectrum resources
  - A paradigm shift in spectrum management (i.e., processes, regulatory, policy) and spectrum access technologies

Policy Issues

Based on the session discussions, the following underlying policy issues should be studied by the NSTAC or an international counterpart:

- Spectrum Management
  - Framework for dynamic spectrum allocation

Roles & Responsibilities

Industry, academia, and Government all have unique roles and responsibilities in funding and advancing national security and emergency preparedness communications R&D:

Academia	• Basic Research • Education and Training Development • Standards
Industry	• Implementation • Productize • Standards • Funding
Government (Fed, State, local)	• Standards • Policy • Funding • Governance
Others? (Int'l Community)	• Global Collaboration

Priority Areas for Consideration

Members of the emerging technologies breakout session identified the following priority areas for consideration for further R&D:

- **Trusted Architecture**
  - Research required to develop a security model
- **Distributed/Portable Energy Technology**
  - Explore battery technologies to support mobile requirements
- **Assured Attribution**
  - Enhanced attribution techniques
- **Dynamic Spectrum Access**
  - R&D funding to bring DSA to maturity; sponsorship from senior leaders;
  - Integration of existing architecture requiring a migration strategy
  - Policy, technology, and regulatory implications

Speaker Biographies

Speaker and Facilitator Biographies

Ms. Susan Alexander is the Chief Technology Officer (CTO) for Information and Identity Assurance (I&IA), the senior executive within the Office of the Assistant Secretary of Defense (OASD), Networks and Information Integration/ Department of Defense (DOD), Chief Information Officer responsible for integrating technology-based initiatives into the corporate strategy for I&IA. As CTO, she provides a vision for and counsel on how I&IA technology will enable net-centric operations, and fosters initiatives which enhance the Department's ability to benefit from advances in this technology sector.

Ms. Alexander joined OASD from the National Security Agency (NSA), where she headed the National Information Assurance Research Laboratory, directing research, consulting and design spanning the broad spectrum of information assurance topics. Previously, Ms. Alexander led a diverse set of activities at NSA across its defensive and foreign intelligence missions, serving as Technical Director for Counter-Terrorism, Deputy Chief of Cryptographic Evaluations and Chief of Cryptanalytic Attack Development.

Ms. Alexander graduated magna cum laude from Yale University, and then trained as a cryptanalyst, specializing in the diagnosis of cryptographic systems from cipher, and achieved the rank of Master in NSA's technical track. During her years as a practicing cryptanalyst, Ms. Alexander served a tour of duty at NSA's British counterpart agency and authored numerous prize-winning internally-published technical papers (five, in all).

Mr. Gregory Q. Brown is President and Chief Executive Officer (CEO) of Motorola, Inc. Mr. Brown joined Motorola in 2003 and was elected to the company's Board of Directors in 2007.

Prior to his appointment as CEO, Mr. Brown served as President and Chief Operating Officer of Motorola. Among his many accomplishments, Mr. Brown led the acquisition of Symbol Technologies, Inc., the second largest transaction in Motorola's history. Additionally, Mr. Brown returned Motorola's automotive business to profitability and subsequently led the divestiture of that business to Continental. He has headed four different businesses at Motorola, including the Government and public safety business, where earnings substantially increased under his leadership.

Mr. Brown has more than 25 years of high-tech experience. Prior to joining Motorola, he was Chairman and CEO of Micromuse, Inc., a network management software company. Before that, he was President of Ameritech Custom Business Services and Ameritech New Media, Inc. Before joining Ameritech in 1987, Mr. Brown held a variety of sales and marketing positions with AT&T, Inc.

An active member of the civic and business communities, Mr. Brown was appointed by the White House to serve on the President National Security Telecommunications Advisory Committee (NSTAC) in May 2004. Mr. Brown is also a member of the board of directors for Northwestern Memorial Hospital, World Business Chicago, and the U.S.-China Business Council.

Mr. Brown received his bachelor's degree in economics from Rutgers University and is a member of the Rutgers board of overseers.

Mr. Guy Copeland is Vice President, Information Infrastructure Advisory Programs, with CSC, Federal Sector. He joined CSC in January 1988 and served progressively as CSC's director of program management operations, director of implementation, and deputy project manager for the Treasury Consolidated Data Network. Later he was director of the Network Engineering Center.

Mr. Copeland represents CSC's CEO, Mr. Van Honeycutt, in the NSTAC, a body that provides industry advice to the President of the United States, regarding critical, information and telecommunications services supporting our national economy and other critical

functions of society. He currently chairs the NSTAC's Research and Development (R&D) Task Force, which organizes the R&D Exchange Workshop.

In the early 1990's, Mr. Copeland championed an NSTAC initiative that was a progenitor for the "information sharing and analysis center" (ISAC) concept recommended by the President's Commission on Critical Infrastructure Protection. He helped found and also serves as CSC's member on the Board of Directors of the Information Technology (IT) ISAC where he recently completed a term as President. Mr. Copeland was elected, in January 2006, by the membership of the newly created IT Sector Coordinating Council (SCC) to be its first Chairman. Within the IT Association of America (ITAA), he has been a champion for information security and critical infrastructure protection for many years and co-chaired ITAA's Information Security committee for three years. He is also the Co-Vice Chair of ITAA's Homeland Security Committee.

Mr. Copeland chaired the Armed Forces Communications Electronics Association (AFCEA) symposium on critical infrastructure protection in 1998, 1999, and 2000. In 2000, he was the industry co-chair for a government and industry consortium that provided significant recommendations to the Deputy Secretary of Defense on "Information Security for Electronic Business." At the Center for Strategic and International Studies, he contributed to reports with recommendations in the area of cyber threats, cyber crime, and critical infrastructure protection. In 2005, he was named a Senior Fellow at the Homeland Security Policy Institute of George Washington University. He has led and participated in numerous other government and industry collaborative efforts.

Before CSC, Mr. Copeland's United States Army career covered a wide variety of assignments, including research and development projects; organizations responsible for fielding, operating, and maintaining communications systems; a tour in Vietnam as a helicopter pilot; and Military Assistant to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) for the Joint Tactical Information Distribution System.

Mr. Copeland is a senior member of the Institute of Electrical and Electronic Engineers (IEEE). In 1983-84, he was an IEEE Congressional Science Fellow in the office of Senator John Warner (R-VA). He received the 1999 Award for Excellence in information technology from AFCEA International. He earned a master's degree in electrical engineering from the University of California, Berkeley and a bachelor's degree in electrical engineering from the University of Wisconsin, Madison.

Mr. Gregory T. (Greg) Garcia was appointed by Secretary Michael Chertoff on September 18, 2006, to be America's first Assistant Secretary for Cyber Security and Telecommunications (CS&T) for the Department of Homeland Security (DHS), within the Preparedness Directorate. Mr. Garcia leads the strategic direction of CS&T and oversees both the National Cyber Security Division and the National Communications System (NCS).

Prior to joining the Department, Mr. Garcia served as Vice President for Information Security Programs and Policy with ITAA. In this capacity, he managed all programmatic and public policy aspects of information security, with a view to strengthening our national cyber readiness among the user and vendor communities. Additionally, he worked with DHS to co-found the National Cyber Security Partnership.

Before joining ITAA in April 2003, Mr. Garcia served on the staff of the House Science Committee where he was responsible for industry outreach and legislative issues related to information technology and cyber security. In particular, Mr. Garcia played an active role under the leadership of Chairman Sherwood Boehlert (R-NY) in the drafting and shepherding of the *Cyber Security R&D Act of 2002*.

Prior to his experience on Capital Hill, Mr. Garcia worked for several organizations on policy issues. He served as Director of 3Com Corporation's Government Relations Office in Washington, DC where he was responsible

for all aspects of the company's strategic public policy formulation and advocacy. He also served as Coalition Manager for Americans for Computer Privacy, a high profile grassroots policy advocacy campaign dedicated to overturning U.S. export and domestic use regulation of encryption technology. This effort was successful after just one year of intense lobbying and high-end media strategies.

Mr. Garcia lobbied international trade policy for the American Electronics Association, including export controls, customs, European and multilateral trade negotiations. He also worked for Newmyer Associates, Inc. a public policy consulting firm where he reported and consulted on international trade policy for Fortune 500 clients.

Mr. Garcia is a graduate of San Jose State University in California.

Dr. Chris Greer joined the National Coordination Office from the National Science Foundation (NSF), where he served as Program Director for the Office of Cyberinfrastructure and was responsible for strategic planning for digital data activities. He has also served as Program Director in the Directorate for Biological Sciences and Cyberinfrastructure Advisor in the Office of the Assistant Director for Biological Sciences and Executive Secretary for the Long-lived Digital Data Collections Activities of the National Science Board. He currently serves as Co-Chair of the Interagency Working Group on Digital Data of the National Science and Technology Council, Committee on Science.

Dr. Greer received his Ph.D. in biochemistry from the University of California, Berkeley and did his postdoctoral work at CalTech. He was a member of the faculty at the University of California at Irvine in the Department of Biological Chemistry for approximately 18 years where his research on gene expression pathways was supported by grants from the NSF, National Institutes of Health, and the American Heart Association. During that time, he was founding Executive Officer of the RNA Society, an international professional organization with more than 700 members from 21 countries worldwide.

Mr. Gary Grube is a Motorola Senior Fellow in the Government and Public Safety business. Previously he led all wireless research at Motorola Labs and before that held the CTO, and Corporate Vice President position at Motorola's Government and Enterprise Mobility Solutions Business.

Mr. Grube has worked in the area of wireless solutions development focusing on system architecture, key enabling technologies, intellectual property rights, and technology planning. He is credited with the innovations that enabled the first mission critical Internet protocol networks in public safety, the first digital radio systems, and more recently broadband access and applications platforms.

Mr. Grube was recognized with the Dan Noble Fellow award, Motorola's highest recognition for technical achievement. He holds over 100 issued U.S. patents and has many more pending. A frequent public speaker, Mr. Grube has been called upon many times by the U.S. Congress to testify as an expert in matters related to homeland security communications. As a result, new spectrum allocations have been established for the public safety industry such as 700 MHz and 4.9 GHz.

Mr. Grube serves as the Chairman of Safe America, a non-profit organization focused on personal safety awareness and training. In 2003 Mr. Grube was appointed by Mayor Richard M. Daley to serve on the Mayor's Council of Technology Advisors for the City of Chicago promoting high-tech around the Chicagoland area. He is also a member of the Executive Advisory Board of the International Engineering Consortium.

Mr. Grube earned a bachelor's degree in electrical engineering at the University of Illinois, Champaign, a master's degree in Electrical Engineering from the Illinois Institute of Technology, Chicago, and he also holds an MBA earned in the executive program at Northwestern University in Evanston Illinois.

Mr. James J. Madon is the Director and Deputy Manager of DHS's NCS. He is responsible for the day-to-day policy, technical, and programmatic oversight in

coordination of all Federal government-wide activities in national security and emergency preparedness communications. He became the NCS Director and Deputy Manager on April 28, 2008.

Mr. Madon's experience includes development of force control applications and base level data processing for the Air Force Strategic Air Command. While at Bell Laboratories, he focused on telecommunications development, system engineering and governmental projects.

Mr. Madon received his first patent while at Bell Laboratories. He served as an Engineering Manager at Motorola, working a wide variety of areas ranging from wireless data, analog and digital trunking, cellular [time division multiple access and code division multiple access (CDMA)], and in wireless research on cognitive radio topics. He received his second patent for a self synchronizing wireless pilot-less protocol while at Motorola. He was a Director of Call Center Technology at Ameritech, and a product manager at Alcatel-Lucent for 3rd Generation wireless products. He received his third patent for a method and apparatus for detecting the reduction in capacity for CDMA cellular systems while at Lucent.

Madon was recalled to active duty in response to the September 11, 2001 events and retired from the U.S. Air Force Reserves with over 30 years commission service. From March 2005 through April 2008, he served as the Program Executive for Regulatory and Domestic Affairs with the National Aeronautics and Space Administration Headquarters in Washington.

Mr. Madon was born in a suburb of Chicago, entering the U.S. Air Force in 1973 after receiving his commission through the Reserve Officers Training. He has a bachelor's degree in Mathematics from Bradley University, Peoria, Ill., a master's degree from Central Michigan University, Mt. Pleasant, Mich., and a MBA from the University of Chicago, Chicago, Ill.

Mr. Doug Maughan is a Program Manager for cyber security research and development within DHS's, S&T Directorate. Prior to his appointment at DHS, Dr. Maughan was a Program Manager in the Advanced Technology Office of the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia.

His research interests and related programs were in the areas of networking and information assurance. Prior to his appointment at DARPA, Dr. Maughan worked for NSA as a senior computer scientist and led several research teams performing network security research.

Dr. Maughan holds a bachelor's degree in Computer Science and Applied Statistics from Utah State University, a master's degree in Computer Science from the Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County.

Dr. Veena Rawat is the President of the Communications Research Centre Canada (CRC). An agency of Industry Canada, CRC is responsible for conducting applied research and development in communications and related technologies.

During her 28 years of experience with Industry Canada in managing programs related to spectrum engineering, Dr. Rawat led Canadian delegations and negotiations at the International Telecommunication Union, the Organization of American States, and with the United States Government. She was also Co-Chair of the Canada/U.S. Committee to negotiate spectrum use along the border.

Dr. Rawat has chaired many technical committees of Canadian and international organizations that deal with radio, spectrum, and telecommunications issues and standards. In 2003, she became the first woman to chair the World Radiocommunication Conference (WRC) of the United Nations' telecommunication organization for which she was awarded a gold medal by the Secretary General of the ITU.

Her work has garnered her much recognition, including the Canadian Women in Communications Woman of the Year Award in 2004, the International Leadership in Government Award from the Wireless Communications Association International in the

United States, and the Trailblazer award from the Women's Executive Network, which was announced in its list of Canada's Most Powerful Women: Top 100.

Dr. Rawat was the first woman to graduate with a Ph.D. in Electrical Engineering from Queen's University in 1973. She continues to be involved in activities to increase the number of women in science and technology.

Mr. Richard M. Russell is Associate Director of the Office of Science and Technology Policy (OSTP) in the Executive Office of the President. In that capacity Mr. Russell serves as OSTP's Deputy Director for Technology and is responsible for running OSTP's Technology Division and chairing the National Science and Technology Council's Committee on Technology. He was nominated by the President and confirmed by the Senate in August of 2002. Additionally, the President appointed him to serve as the United States Ambassador to the 2007 WRC.

In October of 2007, Ambassador Russell led a delegation of more than 150 government and private sector delegates to the month-long treaty writing conference in Geneva, Switzerland. The WRC is convened every four years under the auspices of the ITU to review and revise the international rules governing the use of radio frequency spectrum and satellite orbits.

Prior to heading the U.S. Delegation to the WRC, Mr. Russell served as Senior Director for Technology and Telecommunications for the National Economic Council. In that capacity he coordinated technology and telecommunications policy for the White House.

Mr. Russell began his tenure in the Bush Administration in 2001 as OSTP's Chief of Staff. Prior to joining the Bush Administration, he spent over a decade on Capitol Hill, working in both the U.S. House of Representatives and U.S. Senate.

From 1995-2001, Mr. Russell worked for the House Committee on Science. During his time on the Committee, he was charged with overseeing the Committee's technology policy, coordinating its oversight agenda, and helping manage the Committee's majority staff. Mr. Russell helped draft a wide variety of legislation, including efforts to expand and improve coordination of federal information technology related agencies. He joined the Science Committee as a professional staff member. He then became Staff Director of the Subcommittee on Technology and finally Deputy Chief of Staff for the full Committee.

Mr. Russell also ran the Washington office of a trade association. He began his career in Washington as a Research Fellow for the non-profit Conservation Foundation.

In 1988 he earned a bachelor's degree from Yale University.

Ms. Leslie Anne Sibick is the Chief of Research and Development Analysis for the Office of Infrastructure Protection (OIP). The R&D Analysis Branch acts as a critical liaison between DHS OIP Infrastructure and Analysis and Strategy Division and OIP staff and the DHS S&T Directorate. This Branch leads the full spectrum of OIP initiatives on behalf of National Infrastructure Protection Plan partners to support S&T Integrated Product Teams, research centers, Centers of Excellence, interagency, and international critical infrastructure efforts.

Ms. Sibick in 2003 joined the Department of Homeland Security Office of the Inspector General, where she led evaluations of emergency preparedness and response programs, and federal grant programs funding first responder equipment, training, and exercises. Ms. Sibick's career includes work in the Homeland Infrastructure Threat and Risk Analysis Center within DHS where she was responsible for a team of analysts conducting national-level fusion of intelligence and critical infrastructure threat and risk information for numerous critical infrastructures.

Ms. Sibick was the Sector Specific Agency Representative, and Sector Specialist, for the Emergency Services Sector within OIP, where she was responsible for providing senior federal representation to and coordinating with the Emergency Services Sector owners and operators. Additionally, she chaired the Emergency Services Government Coordinating

Council, a forum for all federal emergency service agencies to implement Administration objectives. Prior to joining DHS, Ms. Sibick supported the Combating Terrorism Technology Program within the Defense Threat Reduction Agency. Ms. Sibick also has worked for local government and the Department of the Army.

Ms. Sibick attended masters programs in both Business and Biodefense, and she holds a bachelor's degree in Business Administration. She completed the Leadership for a Democratic Society program at the Federal Executive Institute, and Executive Education at Harvard University's John F. Kennedy School of Government.

Acronym List

Acronym List

ACI	American Competitiveness Initiative
AFCEA	Armed Forces Communications Electronics Association
BAA	Broad Agency Announcement
BGP	Border Gateway Protocol
CEO	Chief Executive Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CI/KR	Critical Infrastructure/ Key Resources
CRC	Communications Research Centre
CS	Computer Science
CSIA	Cyber Security and Information Assurance
CTO	Chief Technology Officer
CNCI	Comprehensive National Cybersecurity Initiative
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DND	Department of National Defence
DNS	Domain Name System
DNSSEC	Domain Name System Security
DSN	Defense Switched Network
DOD	Department of Defense
DRDC	Defence Research and Development Canada
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FY	Fiscal Year
GE	General Electric
GETS	Government Emergency Telecommunications Service
GPS	Global Positioning System
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronic Engineers
IES	Industry Executive Subcommittee
IESO	Independent Electricity System Operator
IdM	Identity Management
IIS	Information Infrastructure Security
ISAC	Information Sharing Analysis Center
IP	Internet Protocol
ISP	Internet Service Providers
IT	Information Technology
ITAA	Information and Technology Association of America
ITU	International Telecommunication Union
LMR	Land Mobile Radio
NASA	National Aeronautics and Space Administration
NCE	Networks Centres of Excellence
NCO	National Coordinating Office
NCO/NITRD	National Coordinating Office for Networking and Information Technology R&D
NCRCG	National Cyber Response Coordination Group
NCS	National Communications System
NCSD	National Cyber Security Division
NECP	National Emergency Communications Plan
NGN	Next Generation Network
NII	Networks and Information Integration
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NITRD	Network Information Technology Research and Development
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
OASD	Office of the Assistant Secretary of Defense
OIP	Office of Infrastructure Protection
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
OSTP	Office of Science and Technology Policy
PCAST	President's Advisory Council of Advisers on Science and Technology
PITAC	President's Information Technology Advisory Committee
PREDICT	Protected Repository for Defense of Infrastructure against Cyber Threats
R&D	Research and Development
RDTF	Research and Development Task Force

RDX	Research and Development Exchange
RTAP	Rapid Technology and Prototyping
SBIR	Small Business Innovative Research
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Councils
SDR	Software Defined Radio
SEMATECH	Semiconductor Manufacturing Technology
SME	Subject Matter Experts
SISA	Systems Integration, Standards, and Analysis
SPRI	Secure Protocols for the Routing Infrastructure
S&T	Science and Technology
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity
WiMAX	Microwave Access
WPS	Wireless Priority Service
WRC	World Radiocommunications Conference

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic

November 6, 2008

Table of Contents

Executive Summary

The Federal Government has long recognized the importance of the delivery of national security and emergency preparedness (NS/EP) traffic regardless of the condition of and circumstances surrounding the communications networks. Over the past several decades, the President's National Security Telecommunications Advisory Committee (NSTAC) has provided guidance on how to prioritize NS/EP traffic in times of crisis. Specifically, the NSTAC's industry partners developed recommendations to the President regarding NS/EP communications traffic prioritization that prompted the Department of Homeland Security's (DHS) National Communications System (NCS) to create the Nation's current priority service programs—Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS). With these services, NS/EP users have a high probability of completing calls even during times of network stress.

Service providers have invested billions of dollars to both transform and augment their circuit-switched networks to incorporate the use of technologies based on Internet protocol (IP). As the core networks universally evolve from circuit-switched to packet-based service technologies, it is important for the Federal Government to consider the impact of this evolution on the delivery of NS/EP communications traffic.

Although the rapid growth of the Internet has led to exciting new services for customers, such as Voice over IP (VoIP), these technological advancements have also altered the NS/EP priority-services network environment. To address the need for the continued delivery of NS/EP traffic over packet-based networks, during the 2007 NSTAC Meeting, the Assistant to the President for Homeland Security and Counterterrorism requested that the NSTAC examine concerns regarding the risk, if any, to IP-based NS/EP communications traffic, including VoIP, during times of perceived abnormal conditions or network duress. Specifically, the White House requested that the NSTAC determine if network degradation or disruption could affect the receipt or delivery of NS/EP traffic and, if so, asked that the NSTAC provide recommendations to the President regarding measures to ensure the delivery of IP-based NS/EP traffic during times of network duress.

To conduct its analysis, the NSTAC examined how service providers transport IP-based traffic across their networks and how they shared data regarding their ability to manage traffic end-to-end. The NSTAC also examined how carriers and service providers offer managed services to meet the requirements of their enterprise customers, including some NS/EP authorized users. After completing its examination, the NSTAC found:

- The core networks are universally evolving from circuit-switched to packet-based service technologies. The network management principles employed by the carriers evolve as the technology of the networks advances, including the ability to manage traffic within and across IP-based network overlays.

- The growth of high-bandwidth applications has led to higher traffic levels and could affect NS/EP communications traffic. Service providers design and manage their networks to avoid or minimize network congestion and to prevent and respond to network events.

- Enhanced services for NS/EP authorized users in a packet-based network environment must begin with traffic management within customer equipment, such as enterprise routers, servers, and terminal devices, prior to connecting to the service provider/transport portion of the network.

- The public Internet handles packet routing on a best-effort basis, meaning it will try its best to forward user traffic, but can provide no guarantees regarding loss rate, bandwidth, delay, and/or jitter. [1]

- Within a single network via a managed service offering, a service provider can offer performance/reliability assurances because it is able to monitor and manage services on an end-to-end basis. A customer can also enter into an agreement with multiple service

providers to receive a specific quality of service (QoS) from the service providers for a managed service.

- The Federal Government uses managed services to meet its communications needs. NS/EP services could also be provisioned using managed services within the new IP-based environment.

- The Nation's NS/EP capabilities based on the public switched telephone network (PSTN) continue to support key leadership and first responders using GETS, WPS and TSP, but with the increasing consumer and commercial adoption of IP-based communications, its long-term viability is diminishing.

- The NCS is working with industry partners to establish IP-based priority services using an "industry requirements" model, which was previously successful in developing the GETS and WPS solutions. Continued funding for these NCS activities is essential to enable continued Government and industry collaboration and to ensure that advanced NS/EP services are there when needed.

- Global standards bodies are addressing NS/EP IP-based priority services delivery. The United States has an opportunity to influence the outcomes of these standards bodies by actively participating and leading the standards development process.

- The Federal Communications Commission (FCC) found that the provision of priority services offered to NS/EP authorized users was *prima facie* lawful under the *Communications Act of 1934.* These priority services support critical functions such as national security leadership, continuity of government, public health, and safety, maintenance of law and order, and disaster recovery during national security emergencies. This provision must maintain the authority to ensure that networks remain capable of providing priority communications for NS/EP authorized users in the future.

The NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* that the President should:

- In the short term, establish a policy that requires Federal departments and agencies to:

  - Ensure their enterprise networks are properly designed and engineered to handle high traffic volume;

  - Manage traffic through QoS programming in its routers to prioritize traffic, including NS/EP traffic; and

  - Expand the use of managed service agreements to provision NS/EP services within the new IP-based environment.

- In the long term, require that Federal departments and agencies remain actively involved in standards development of priority services on IP-based networks by supporting efforts to:

  - Provide adequate funding that will be used to develop timely solutions across all technology platforms; and

  - Commit appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services.

- Petition the FCC for a declaratory ruling to confirm that network service providers may lawfully provide IP-based priority access services to NS/EP authorized users.

Footnote

1 Jitter is defined as any disruption in packet transmission or delivery.

1 Introduction

1.1 Background

The Federal Government has long recognized the importance of optimizing the delivery of national security and emergency preparedness (NS/EP) traffic regardless of network conditions. Over the past several decades, the President's National Security Telecommunications Advisory Committee (NSTAC) has provided guidance to the President on how to prioritize of NS/EP traffic in times of crisis. As a result of that guidance, the Federal Government now operates three priority programs developed in part by the U.S. telecommunications industry: the Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS). [2] These programs are available to NS/EP authorized users to promote the Nation's security and emergency preparedness functions.

The Government established the existing priority service programs based upon the technologies and interfaces most prevalent at the time they were developed. While past technologies and communications transport mechanisms continue to operate today, the core network transport is universally evolving from circuit-switched to packet-based service technologies. This evolution has helped provide a common operating interface between various access technologies, applications, and providers, including the public switched telephone network (PSTN), private managed networks, and the public Internet.

The Federal Government has begun to prepare for this evolution and to comprehend how the shift to Internet communications and packet-based networks will affect the delivery of NS/EP traffic. Past NSTAC efforts and the ongoing work of the Department of Homeland Security's (DHS) National Communications System (NCS) have analyzed the need for the NS/EP community to keep pace with technology advancements. [3]

1.2 Charge

During the President's 2007 NSTAC Meeting, the Assistant to the President for Homeland Security and Counterterrorism asked the NSTAC to examine concerns regarding the risk, if any, to Internet protocol (IP)-based NS/EP communications traffic, including voice over IP (VoIP), during times of perceived abnormal conditions or network duress. Specifically, the White House requested that the NSTAC determine if network degradation or disruption could affect the receipt or delivery of NS/EP traffic and, if so, provide recommendations to the President regarding measures to ensure the delivery of IP-based NS/EP traffic during those times of network duress.

1.3 Process

The NSTAC examined how service providers transport IP-based traffic across their networks. Several member companies shared information regarding their companies' end-to-end traffic management and routing procedures. They also discussed the solutions their companies use to meet the communications needs of customers. The NSTAC members evaluated strategies and policies guiding how inter-carrier IP-based traffic is transported end-to-end. Furthermore, representatives from Federal agencies briefed the members regarding the evolution of IP-based network infrastructures, the related potential risks, and the standards and technical requirements needed to provide NS/EP authorized users with future IP-based priority services.

Appendix A lists the task force members, industry subject matter experts, and Government participants who contributed to this effort.

2 Network Evolution

The global communications architecture is a complex collection of networks, each owned and operated by individual service providers. Technologies are evolving at a rapid pace, increasing the number of options for service providers and customers. The core network is evolving from circuit-switched to IP-based and delivers traffic across the public switched telephone network, private managed networks, and the public Internet. Modern digital technology has allowed the different communications service segments, such as broadcast, cable, satellite, wireless, and wireline, to have common characteristics, such as IP. [4] Service providers have invested billions of dollars to both transform and augment their circuit-switched networks

to incorporate the use of IP-based technologies. This investment enables an increasing number of users to exchange an increasing volume of information via both wireless and wireline devices.

Network transport technology is universally standardizing upon IP, a network-layer protocol that contains addressing information and some control information to enable packet routing in networks. IP-based networks, through their flexible, packet-based architecture, inherently can perform many basic functions that a switched or provisioned circuit network cannot do, such as provide more efficient use of bandwidth since it is not a connections-based architecture and simultaneously exchange data to/from remote entities. These fundamental capabilities provide the opportunity to expand the use of networking. The transport layer encompasses the physical and link layers of the IP protocol model. Appendix C discusses some of the major technologies associated with the transport layer.

Service providers continue to implement innovative access, switching, and transport technologies, as well as customer premise equipment along with integrating enhanced multiplexing and packet protocols. Carriers also employ technologies that provide the quality of service to which users have become accustomed. These new technologies and architectures must also work with legacy systems and equipment. It is inevitable that telecommunications networks will continue to evolve as new technologies are developed and advanced network elements are incorporated. It is critical that the network continue to perform in the time of a national emergency just as it is essential for service providers to ensure that network improvements keep pace with user demands to exchange information.

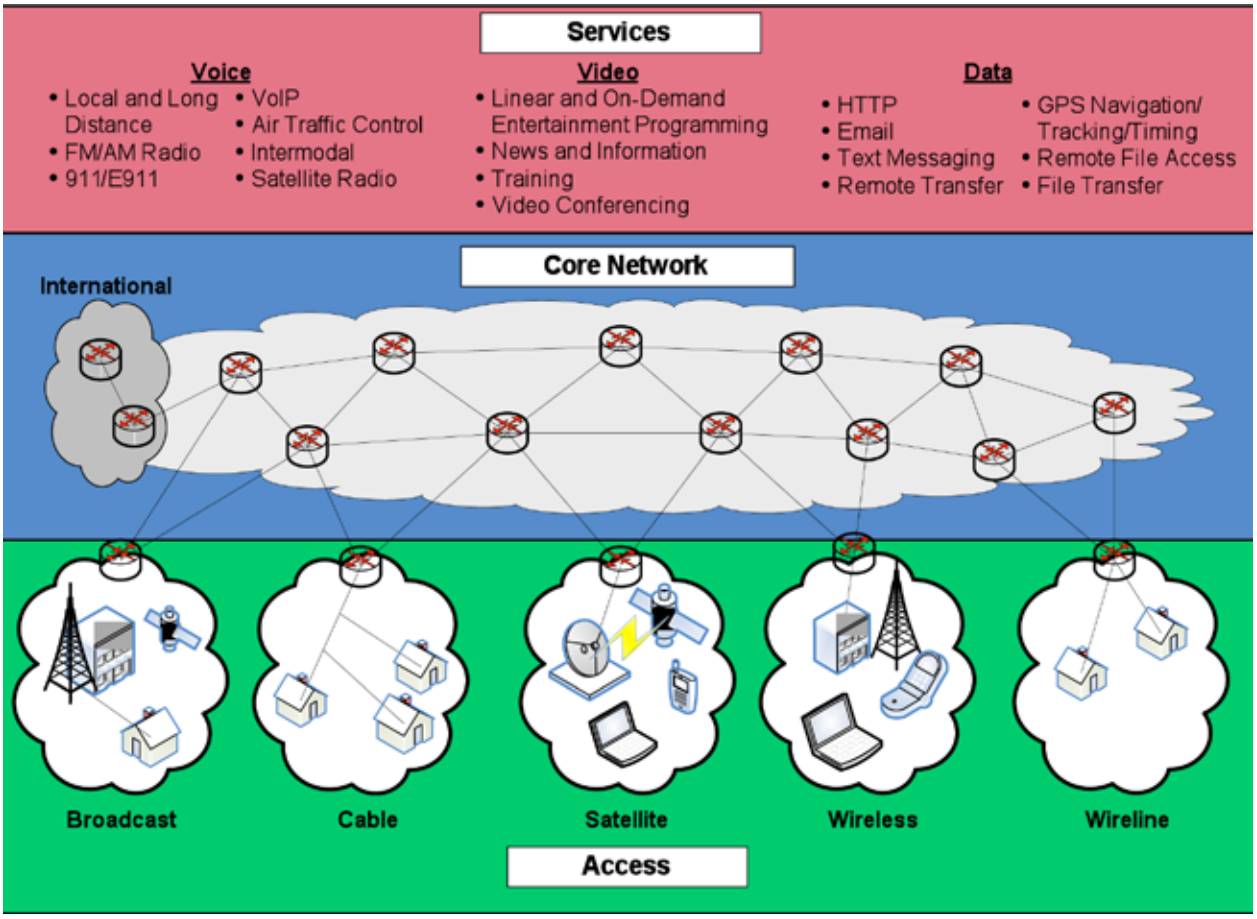


Figure 1 Communications Sector Architecture Model [6]

Additionally, NS/EP authorized users must be aware of the advancements in telecommunications networks as communications needs evolve and expand. Many service providers offer their customers IP-enabled, applicationaware, managed services to deliver security, flexibility, and performance levels for their intranet solutions on a global basis. In addition, to avoid single points of service failures, it is important that NS/EP authorized users discuss their needs for highly reliable access connections with their service provider. These requirements should include diverse routing paths, as well as diverse technologies to access the network where available. [5] Figure 1 depicts the diverse services and technologies that service providers offer over the networks.

3 Network Management

Network management is a key requirement to optimize successful operations in both the circuit-switched and packet-switched network environments. Network management techniques evolve as network technology advances, including the ability to manage traffic within and across IP-based network overlays. While managing networks, providers monitor traffic flow and performance to optimize data flow across the network for all users. Network management for IP networks includes monitoring the network for service failures and down ports; service degradation, including packet delay/loss and jitter; traffic anomalies, such as border gateway protocol routing anomalies; and congestion conditions. For circuit-switched voice communications, network management involves responding to incidents such as blocked voice calls during an unusual mass calling event or congestion caused by reduced capacity due to out-of-service conditions, such as trunk connectivity. [7]

In order to optimize network traffic flow, carriers have developed several processes to manage network voice traffic. These processes, based upon network management principles, include:

- Utilizing all available resources;
- Continuous monitoring of traffic volumes and facility utilization;
- Giving priority to connections that make the most efficient use of network resources, in the case of overload; and
- Inhibiting traffic congestion and preventing its spread.

It is critical for telecommunications service providers to be able to manage NS/EP traffic at the time of a national emergency or other event. The growth of high-bandwidth applications has led to higher traffic levels that could affect NS/EP communications traffic. Service providers have historically managed traffic volumes and characteristics in order to provide good performance to customers, including the Government. As newer network technologies call for modified management techniques, effective traffic management will require service providers to continuously monitor networks and traffic flow and take necessary steps to ensure the minimization of network congestion on a day-to-day basis and/or during a national emergency. Enhanced services for NS/EP users in a packet-based network environment must begin with traffic management within the customer equipment, such as enterprise routers, servers, and terminal devices, prior to connecting to the service provider/transport portion of the network.

3.1 IP Routing

The public Internet is comprised of a worldwide commercial collaboration of tens of thousands of individual networks managed by unaffiliated service provider networks using IP to facilitate user-to-user communications. The public Internet uses a structured addressing system through an IP address registry service, that has a standardized language or protocol for communicating between networks; and adheres to a wide array of other technical agreements, such as the ability to translate alphanumeric domain names (e.g., www.dhs.gov) into IP addresses through domain registry services and a hierarchical Domain Name System (DNS) infrastructure. This voluntary collaboration permits any individual device connected to the public Internet to interact with another connected device or application anywhere in the world. [8]

Internet service providers (ISP) provide the means to connect a physical location to the public Internet as well as provide the ability to connect to other networks participating in the public Internet. In order for its customers' traffic to reach other ISPs' networks, the ISP must establish a business relationship with one or more other network service providers. Such arrangements, called transit and peering agreements, allow one network to hand off traffic destined for another network. Transport networks are rarely universal and data must therefore use a series of networks to get from its origination point to the end destination. Transit service enables small networks to reach the Internet via larger backbone networks.

Peering traffic between the largest networks occurs via signed peering agreements. The individual policies set by each ISP establish the framework for peering agreements, typically based on a relationship of mutual benefit. Peering agreements provide benefits to both ISPs and give them greater control over the routing of their traffic, as the agreements reduce the costs of transporting traffic between networks and help traffic flow more efficiently. Many of these peering connections occur within commercial carrier-neutral third party exchange points, also called carrier hotels. Within these sites, ISPs and others may choose to interconnect and transmit traffic in instances when a policy agreement is not in place.

Since thousands of unaffiliated networks may deliver IP packets across the Internet, attempts to provide consistent quality of service (QoS) treatment would require network providers to coordinate service offerings, network design and engineering, and operational practices. [9] Such agreements generally do not exist today. QoS is a method for network operators to manage traffic, group together the packets generated by different applications with similar performance requirements, and treat the grouping as a family, or flow class, within a network. The public Internet IP routers make no distinction in how packets are processed, meaning that all packets will receive the same QoS. As such, the public Internet handles packets on a best-effort basis, meaning it cannot provide a guarantee regarding loss rate, bandwidth, delay, and/or jitter. [10]

3.2 Congestion

IP networks transmit data in IP packets. Each IP packet includes both a header that specifies source, destination, and other information about the traffic and the message data itself. Network congestion in the IP network environment occurs when the amount of traffic carried by a link or node exceeds its capacity and results in a deteriorated quality of service level, such as packet delay or loss. [11] With non-delay sensitive applications, such as e-mail or instant messaging, the effects of packet delay or loss on the IP network are likely unnoticed by the end user. [12] For delay-sensitive applications, such as VoIP, real-time gaming, or IP television, packet delay or loss can affect the application's ability to operate or its service quality. Service providers, however, have the ability to design and manage their networks to avoid or minimize network congestion and to prevent and respond to network events.

The user will experience network performance that is only as good as the service provider's slowest link. Congestion can occur in many places along a user's communications path. A congested edge, enterprise, or customer premise router can reduce bandwidth and lead to packet loss. Congestion can also occur in a network node, such as a router or switch, from traffic aggregation in which traffic from multiple input ports is destined for a single output port. Network nodes buffer and place traffic exceeding the line speed of the output port in a queue. Waiting in the queue will add delay to the traffic and overfilling the queue will lead to packet loss and degraded application performance. A router placed at the edge of the network to connect various types of residential, cellular, satellite, or enterprise clients to the core network may experience congestion at peak traffic times or during network events. At such times, it may not be able to attain the optimum data transfer speeds if congestion occurs in a router as packet buffers reach capacity. Congestion in edge routers has the potential to affect adversely the performance of applications that depend on the routers to function effectively. This is also true for the edge router at the receiving end. When routers receive more inquires than they have the ability to handle, the user may experience a delayed response. Service providers strive to manage capacity on edge router

resources so that users do not experience congestion where their traffic enters the network. Appendix D provides examples of where congestion may occur across the network.

In order to help reduce the effects of network congestion on delay-sensitive applications, a customer can place a fully managed QoS router in its premise. The QoS router employs a robust set of mechanisms to identify voice traffic (inbound or outbound) and ensure that the required amount of bandwidth is available. Additionally, a simple, highly reliable approach to reduce the possibility of network congestion is for service providers to provision a dedicated connection from the customer premises to the IP network edge with bandwidth sufficient to preclude any potential congestion.

4 Applications

As networks have evolved, so too have the supporting operations support systems, software programs, and databases, which have become crucial in their support of the ability to exchange information. The Government, corporations, and consumers rely on systems and supporting databases for a myriad of uses. As applications continue to grow, so does the demand those applications place on the network. Every application (e-mail, instant messaging, data and file sharing, streaming video, VoIP, etc.) uses capacity on the network to exchange information. Time sensitive applications, like voice and video, place additional performance requirements on the network such as limits on propagation, delay, jitter, and packet loss.

VoIP is one example of an application that uses IP packet-based technologies. When a customer uses a VoIP-equipped device, the device converts the call into a digital format, dividing the message into individual IP packets for transmission, and transmits the IP packets across a public or private network. Currently, the majority of callers utilize circuit-switched based technology; because of this, VoIP calls frequently must also traverse circuit-switched networks to connect to users who do not use VoIP-equipped devices and therefore remain on the circuit-switched network. However, as the number of business and residential IP telephony subscribers increase, end-to-end IP calls will also increase in number. In the interim, IP providers are interconnected through circuit-switched providers via peering arrangements.

VoIP services today are typically provisioned either via best-effort routing over the public Internet or via managed services. With the first service, the provider uses the Internet to route the calls to an external voice telephone switch, normally hosted at a traditional central office or similar facility. With this approach, there is a potential single point of failure where the organization's router interfaces with the upstream ISP.

Using managed services, an internal IP private branch exchange (PBX) handles telephone calls on the enterprise local area network (LAN), bringing them out of the organization via a traditional PBX or other voice switch. The advantage to this approach is that there are now two possible paths for a phone call, a primary path through the PSTN and a secondary path through the Internet as is done in the first option above.

In both cases, the VoIP phones use the same LAN infrastructure as the desktop workstations, thus saving on the cost of having a second parallel-wired telephone infrastructure. Some VoIP products use only the public Internet to route voice calls, and depend on end-to-end routing of VoIP packets. Other products have a voice switch or gateway inside the customer's premise that takes the VoIP packets off the LAN and connects them to the PSTN as though they were traditional analog or digital voice calls. NS/EP authorized users should carefully consider the reliability, security, and performance of best efforts routing across the public Internet as a transport path versus the use of traditional PSTN or managed networks as a transport path. Additionally, NS/EP authorized users should consider using managed services as detailed in the section below.

5 Managed Services

Carriers and service providers typically offer managed services as an integrated, "packaged" solution to meet the requirements of enterprise customers. This can include communications and network services with integrated provisioning and operations management, application hosting and management services, data

processing and storage services, mobility solutions, business continuity solutions, or combinations thereof. These offerings frequently include "private" communications capabilities through means such as dedicated circuit paths, software defined networks, and virtual private networks (VPN). Managed services are private communications because they provide only connections between certain points that the customer authorizes or is dedicated to delivering a particular type of capability. Managed communications services address the need for communications' security, separation, and resilience at significantly lower cost than construction of a unique, dedicated network.

With a high degree of collaboration with its customer, a service provider can keep mission-critical data networks carrying both voice and data traffic running successfully during network anomalies or instances of congestion. Managed services are reliable, secure, and cost-effective solutions that take advantage of converged infrastructure.

Within a single network, a service provider can offer performance/reliability assurances because it is able to monitor and manage services on an end-to-end basis. When the customer first contracts services, the customer and service provider can devise a contractual service level agreement (SLA) to define the QoS flow classes and the performance within a specified range of parameters, including availability, latency, jitter, and packet loss. The customer and service provider define how to recognize the packets generated by the customer's various applications and specify the mapping of each to a flow class. The parties also reach agreement regarding what will occur if the customer generates more than the agreed-upon volume of flow for a particular class.

In some cases, a customer enters into multiple agreements with individual service providers to receive a specific quality of service within and among service providers. [13] In this instance, the carriers engineer and manage the service to meet the customer's requested QoS for performance and reliability assurances. The customer has the responsibility to mark the traffic per the agreement with each service provider in order for the service provider to recognize the markings and route the traffic accordingly.

A VPN generally takes full advantage of the QoS differentiation options within the service provider's network. It can also use end-point encryption and/or logic in the service provider's network routers to permit traffic to move only between the points authorized by the customer. In this way, the service provider's managed service capabilities delivers performance tailored to the customer's business applications while providing the security business customers seek when using a private network. Furthermore, the use of a common physical infrastructure reduces costs.

Although much of a VPN's traffic may be on one service provider's network, it is possible to enable connections to locations on different service providers' networks, though such connections will typically require encryption to ensure that they are secure. For example, remote access working arrangements may use inter-carrier connections. Because these connections can traverse the public Internet, which involves crossing multiple unaffiliated physical networks, they will not have service assurances. Likewise, it is possible for a VPN to have connections to the public Internet. A public Internet connection, however, would need the protection of firewalls and other security technologies, and the end-to-end connection would not be subject to service assurance.

The Federal Government uses managed services to meet its communications needs. [14] The use of managed services could be expanded to provision NS/EP services within the new IP-based environment.

6 Government and Industry Collaboration

The U.S. Government has long recognized the Nation's increasing reliance on telecommunications services. During times of emergency, crisis, or war, personnel with NS/EP missions must have confidence that they will not lose their access to the priority-enabled services supported by communications providers' networks. For several decades, the Government

and its industry partners have worked to develop the centralized, well-established, and mature set of technical standards and business practices that exist in the PSTN today, supporting a ubiquitous national NS/EP communications capability. The evolving IP-based data networks are highly decentralized and operate in environments where Government and industry have only just begun to address and develop technical specifications and standards.

6.1 Next Generation Network-Based Priority Services

The Nation's PSTN-based NS/EP capabilities continue to support key leadership and first responders, but with an ever-increasing consumer and commercial adoption of IP-based communications, its long-term viability is diminishing. Many agencies and organizations have therefore undertaken next generation network (NGN) NS/EP planning efforts to replace this resource.

Within the public Internet, a best effort treatment of packets cannot guarantee that NS/EP traffic receives end-to-end priority service; therefore, the NCS and its industry partners have examined ways to optimize priority using an "industry requirements" model, with inputs from consultants, equipment vendors, and service providers. [15] This model was previously successful when developing the GETS and WPS solutions. In December 2007, the NCS completed the first of several phases of standards work, laying the foundation for industry to plan for NS/EP service development (i.e., voice, then video and data) within the industry's IP multimedia subsystem architecture. The report, titled *National Security and Emergency Preparedness Internet Protocol Multimedia Subsystem Core Network Industry Requirements for Next Generation Networks Government Emergency Telecommunications Service, Phase 1, Voice Service* includes an analysis of potential call connection combinations and various evolving network architectures. It is important that Congress fund the NCS work in this area to continue industry and Government collaboration and to ensure that advanced NS/EP services are operational when needed.

6.2 Industry Standards

Several global standards bodies are addressing NS/EP next generation IP-based priority services delivery. Standards bodies developing provisions for special handling of priority services to support critical communications in the emerging IP packet-based network environment include:

- The Internet Engineering Task Force
- International Telecommunication Union - Telecommunication Standardization Sector
- Alliance for Telecommunications Industry Solutions
- The European Telecommunications Standards Institute's Telecoms and Internet Converged Services and Protocols for Advanced Networks
- Third Generation Partnership Project

Many countries, including the United States, participate in these bodies to formulate standards for future worldwide adoption. At a time when countries such as China, Japan, and South Korea are becoming more actively engaged in the standard-setting process, it is important that the United States commit appropriate resources to maintain a leadership position. This will help ensure the United States has the opportunity to influence the global adoption and implementation of standards that will drive the long-term effects on IP-based prioritization.

7 Legal and Regulatory Policies

Directed by Presidential Executive Order, [16] the NCS is responsible for ensuring "that a national telecommunications infrastructure is developed which is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies other entities, including telecommunications in support of national security leadership and continuity of government." [17]

In fulfillment of its responsibilities, the NCS manages the TSP and GETS programs, both NS/EP priority services that provide nationwide, ubiquitous voice and voice-band data service in the PSTN. Since 2001, NCS also has managed the WPS, which provides priority NS/EP service in the cellular wireless portion of the PSTN.

In 2000, the Federal Communications Commission (FCC) issued an order establishing that the priority services offered to NS/EP authorized users were *prima facie* lawful under the *Communications Act of 1934* as amended, and not an unreasonable preference or discrimination in contravention of Section 202(a) of the Act. [18] These priority services support critical functions such as national security leadership, continuity of government, public health, and safety, maintenance of law and order, and disaster recovery during national security emergencies.

The authority contained in this FCC precedent must be maintained to ensure networks are capable of providing priority communications for NS/EP authorized users in the future. As explained in this paper, packet-switched-based technology infrastructure carrying higher bandwidth applications continue to replace the PSTN and other legacy circuit-switched networks. As that IP technology becomes more widespread and plays an increasingly important role in supporting NS/EP services, those services—and the network management techniques that make them possible—must be permitted to evolve in an IP-based environment. For that evolution to occur, the proper legal and regulatory policies must be in place to ensure NS/EP traffic continues to have priority treatment on IP-based networks. Consistent with its ruling that priority access services offered by carriers to NS/EP authorized users are "*prima facie* lawful" under the Communications Act and do not constitute "unreasonable discrimination" under section 202 of the Act, [19] the FCC should specifically confirm that the same is true with regard to IP-based priority access services offered by IP-based providers to NS/EP users. [20]

8 Key Findings

The NSTAC finds the following:

- The core networks are universally evolving from circuit-switched to packet-based service technologies. The network management principles employed by the carriers evolve as the technology of the networks advances, including the ability to manage traffic within and across IP-based network overlays.
- The growth of high-bandwidth applications has led to higher traffic levels and could affect NS/EP communications traffic. Service providers design and manage their networks to avoid or minimize network congestion and to prevent and respond to network events.
- Enhanced services for NS/EP authorized users in a packet-based network environment must begin with traffic management within the customer equipment, such as enterprise routers, servers, and terminal devices, prior to connecting to the service provider/transport portion of the network.
- The public Internet handles packet routing on a best-effort basis, meaning it will try its best to forward user traffic, but can provide no guarantees regarding loss rate, bandwidth, delay, and/or jitter.
- Within a single network via a managed service offering, a service provider can offer performance/reliability assurances because it is able to monitor and manage services on an end-to-end basis. A customer can also enter into an agreement with multiple service providers to receive a specific QoS from the service providers for a managed service.
- The Federal Government uses managed services to meet its communications needs. NS/EP services could also be provisioned using managed services within the new IP-based environment.
- The Nation's PSTN-based NS/EP capabilities continue to support key leadership and first responders using GETS, WPS and TSP, but with the increasing consumer and commercial adoption of IP-based communications, its long-term viability is diminishing.
- The NCS is working with industry partners to establish IP-based priority services using an "industry requirements" model, which was previously successful in developing the GETS and WPS solutions. Continued funding for these NCS activities is essential to enable continued Government and industry collaboration and to

ensure that advanced NS/EP services are there when needed.

- Global standards bodies are addressing NS/EP IP-based priority services delivery. The United States has an opportunity to influence the outcomes of these standards bodies by actively participating and leading the standards development process.

- The FCC found that the provision of priority services offered to NS/EP authorized users was *prima facie* lawful under the *Communications Act of 1934.* These priority services support critical functions such as national security leadership, continuity of government, public health, and safety, maintenance of law and order, and disaster recovery during national security emergencies. This provision must maintain the authority to ensure that networks remain capable of providing priority communications for NS/EP authorized users in the future.

9 Recommendations

The NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* that the President should:

- In the short term, establish a policy that requires Federal departments and agencies to:

  - Ensure their enterprise networks are properly designed and engineered to handle high traffic volume;

  - Manage traffic through QoS programming in its routers to prioritize traffic, including NS/EP traffic; and

  - Expand the use of managed service agreements to provision NS/EP services within the new IP-based environment.

- In the long term, require Federal departments and agencies to remain actively involved in standards development of priority services on IP-based networks by supporting efforts to:

  - Provide adequate funding that will be used to develop timely solutions across all technology platforms; and

  - Commit appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services.

- Petition the FCC for a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users.

Footnotes

2 An overview of the GETS, TSP, and WPS programs can be found at the National Communications System's Web site, http://www.ncs.gov/.

3 Some of the related NSTAC work efforts include the 2001 *NSTAC Report on Convergent Technologies* and the 2006 *NSTAC Report on Next Generation Networks.* An example of an NCS-led effort is the *2004 NCS Technical Information Bulletin 04-02, Internet Technologies in a Converged Network Environment.*

4 Additional information on the evolution of the access and core networks is contained in Appendix B.

5 *NSTAC Financial Services Task Force Report,* April 2004.

6 Communications – Sector Coordinating Council's National Security Risk Assessment, May 2008.

7 Additional information regarding network management is contained in Appendix C.

8 As this report was being developed, attack methods for a significant DNS vulnerability were widely publicized. Other NSTAC work will address security issues such as these.

9 Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including frame relay, asynchronous transfer mode (ATM), Ethernet and 802.1x networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

10 Jitter is described as any disruption in packet transmission or delivery.

11 Use of the term "congestion" should not be construed to mean a stoppage of data flow; rather it is a delay in the delivery of packets until sufficient network capacity is available to carry them to a device or application.

12 With these types of services, data can be sent on a "store and forward" basis, meaning that the data is sent when the transmission path is available. Since the action is not real time, the receiver is unaware of the delay.

13 Carriers are working to provide a service within a public network environment where QoS and priority markings are recognized and acted upon throughout the entire network.

14 GSA's Networx Universal and the National Capital Region's Washington Interagency Telecommunications System contracts provide enhanced communications services and are examples of Government's use of managed services.

15 It is also important to note that end-to-end delivery requires the customer to be able to receive the traffic that is delivered to them.

16 In 2007, in the President's National Continuity Policy (NCP), the Secretary of Defense was tasked in coordination with the Secretary of Homeland Security to provide secure, integrated, continuity of Government communications to the President, the Vice President, and certain key executive departments and agencies. In addition, the NCP directed the heads of the executive Departments and Agencies to "plan, program, and budget" for those continuity capabilities. See National Security Presidential Directive 51/ Homeland Security Presidential Directive 20.

17 Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (amended by E.O. 13286 of February 28, 2003).

18 FCC's Second Report and Order - Establishment of Rules and Requirements for Priority Access Service, WT Docket No. 96-86, Adopted July 3, 2000.

19 Id.

20 The FCC previously sought comment regarding services and applications making use of IP and the the impact that IP-enabled services have had and will continue to have on the United States' communications landscape. See Notice of Proposed Rulemaking on IPEnabled Services, WC Docket No. 04-36. DHS filed Comments in response to the NPRM noting that "[a]ll VoIP providers, ISPs and IP transmission carriers should be permitted to provide assured service enhancements (including priority treatment) to NS/EP marked traffic while not providing such enhancements to other traffic." In its comments, DOD also stated that "NS/EP considerations provide a compelling rationale for applying a certain amount of regulation to IP-enabled services. The purpose of such regulation would be to ensure the prioritized availability of certain communication services in times of emergency or national crisis."

Participant List

Task Force Members

AT&T, Incorporated
Mr. Thomas Hughes
Ms. Rosemary Leffler

Bank of America Corporation
Mr. Roger Callahan

Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Juniper Networks, Incorporated
Mr. Robert Dix

Microsoft Corporation
Ms. Cheri McGuire

Nortel Networks Corporation
Dr. Jack Edwards

Qwest Communications International, Incorporated
Ms. Kathryn Condello

Raytheon Company
Mr. William Russ

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Nextel Corporation
Ms. Allison Growney

Telcordia Technologies, Incorporated
Ms. Louise Tucker

Verizon Communications, Incorporated
Mr. James Bean

Other Participants

AT&T, Incorporated
Dr. Bobbi Bailey

Bank of America Corporation
Mr. Larry Schaeffer

Computer Sciences Corporation
Ms. Janet Gunn

European Commission
Mr. Detlef Eckert
Ms. Anna Snow

George Washington University
Dr. Jack Oslund

Juniper Networks, Incorporated
Mr. Tom Van Meiter

Qwest Communications International, Incorporated
Ms. Kathryn Condello
Mr. R. David Mahon
Mr. Thomas Snee

Renesys Corporation
Dr. Earl Zmijewski

Sprint Nextel Corporation
Mr. John Stogoski

VeriSign, Incorporated
Mr. William Gravell

Verizon Communications, Incorporated
Mr. Marcus Sachs

U.S. Government Personnel

Department of Defense
Mr. Anthony Bargar
Ms. Catherine Creese
Mr. Marna Harris
Mr. Herb Herrmman
Capt. John Kennedy
Mr. Mark Lauver
Ms. Hillary Morgan
Mr. Dan Wenk

Department of Homeland Security
Ms. Sue Daage
Mr. Vern Mosley
Mr. An Nyguen
Mr. Frank Suraci
Mr. Will Williams

Executive Office of the President
Mr. Billy O'Brien

Federal Communications Commission
Mr. Richard Hovey

Federal Reserve Board
Mr. Wayne Pacine

Access and Core Networks

Access and Core Networks

Access describes the part of a communications network that subscribers use to connect to their immediate service provider. It refers specifically to the series of physical connection methods that interconnect a consumer/business termination point and its service provider, such as the local exchange carrier, Internet service provider (ISP), or cable television service provider. [21] Access networks are evolving to include fiber optic technology as providers bring the benefits of high capacity and value-added services over broadband networks to customers. To avoid single points of service failures, it is important that national security and emergency preparedness (NS/EP) authorized users discuss their needs for highly reliable access connections with their service provider. These requirements should include diverse routing paths, as well as diverse technologies to access the network where available.

A core network transports a high volume of aggregated traffic over significant distances via fiber optic cable, microwave radio, copper cable, or satellite and interconnects access networks across the country. Core networks span the globe mainly using submarine fiber optic communications cable systems as well as land-based fiber cable networks.

These core networks interconnect at numerous points throughout the Nation, forming the communications infrastructure. Core networks are today primarily composed of terrestrial and undersea wireline networks, with satellite links being an exception. [22] The same core network delivers traffic for the public switched network, private managed networks, and the public Internet. [23] The voice core networks are evolving from circuit switched to packet-based. Service providers deploy self-healing technologies to protect their physical networks, as well as leverage the interconnection of these networks to provide resilience and redundancy to sustain availability during an incident. As discussed in the *NSTAC Report to the President on Network Operations Centers,* service providers operate network operations centers to configure, monitor, and provision the core network nodes. [24] Service providers collect various forms of information about their networks, including statistics, alarms, and utilization data, which are important tools that service providers use to monitor network health and performance and re-route traffic in the event of congestion.

Interconnection agreements or tariff filings outline how to handle the exchange of voice traffic between service providers across the public switched telephone network (PSTN). To meet these obligations, service providers enter into interconnection agreements or file tariffs, which include the transmission and routing of telephone exchange service and exchange access at any technically feasible point within the provider's network. Additionally, service providers are required to establish reciprocal compensation arrangements for the transport and termination of telecommunications. The terms and conditions contained in interconnection agreements outline how providers deliver traffic and compensate one another for the use of their networks. These terms and conditions also outline the steps for dispute resolution should any issue arise.

ISPs interconnect through dedicated connections or at peering points, and establish agreements to exchange or transit traffic. In addition, smaller ISPs may elect to purchase access services from larger, or Tier 1, backbone providers. These interconnections only provide for exchange of "public" Internet traffic. Internet peering generally does not include interconnection of private (e.g., enterprise) or carrier core network traffic or services that include advanced features.

Footnotes

21 The local telephone exchange contains automated switching equipment that directs a call or connection to a consumer.

22 The satellite segment can provide worldwide transport services as well, however the access segments presented within the architecture generally use wireline core networks for sending traffic (though cable and broadcast may receive substantial video feeds via satellite). As a result, core networks generally refer to the wireline core network and specific mention is made of the satellite segment's role as a core network.

23 The public Internet is an application that is delivered over networks and not a network itself.

24 NSTAC Report to the President on Network Operations Centers. February 2008.

Transport Layer

Transport Layer

Multi-Protocol Label Switching

Many service providers make use of the Multi-Protocol Label Switching (MPLS) technology layer in their network infrastructure to provide capabilities and service features beyond that of Internet protocol (IP) alone, such as complex network traffic engineering and sharing same network infrastructure amongst Internet access services and secured virtual private network (VPN) services. Use of this technology enables carriers to achieve economy-of-scale and lower unit cost. IP routing protocols have no awareness of the capabilities and characteristics of the underlying physical network. MPLS addresses this limitation by enabling the handling of IP packets based on mapping the packets to a flow class. These flow classes can utilize predetermined edge-to-edge paths that have predictable performance characteristics, as compared to the hop-by-hop, best available route handling inherent with public Internet routing. Packet mapping occurs each time a customer's IP-based router sends traffic into the MPLS network.

At the entry point to the MPLS network, the network encases the IP packet in a new envelope called a label and directs it to the far side of the MPLS network, based on the edge MPLS router associated with the destination IP address. The logic for routing across the available bandwidth is a function of the flow class of the MPLS packet. At the far edge, the MPLS removes the envelope, revealing the original IP information. A service provider that employs MPLS and supports the public Internet usually uses a single flow class for all traffic directed to or coming from the public Internet. This flow class will not have any assured level of performance. This is consistent with the treatment of all public Internet traffic.

MPLS enables the service provider to define classes of service, also known as quality of service (QoS), across their networks so that the treatment of customers' traffic is different depending upon the application and its performance requirements. For example, VoIP is a delay-sensitive application and business customers typically choose to give VoIP the best treatment or highest QoS that the carrier offers. Carriers offer service level agreements to managed services customers based on the traffic performance characteristics as defined by each QoS.

The diagram below illustrates how the assignment of various flow classes using the QoS functionality of MPLS gives IP traffic priority. Carriers mark packets to ensure the packets receive the correct QoS across the network.

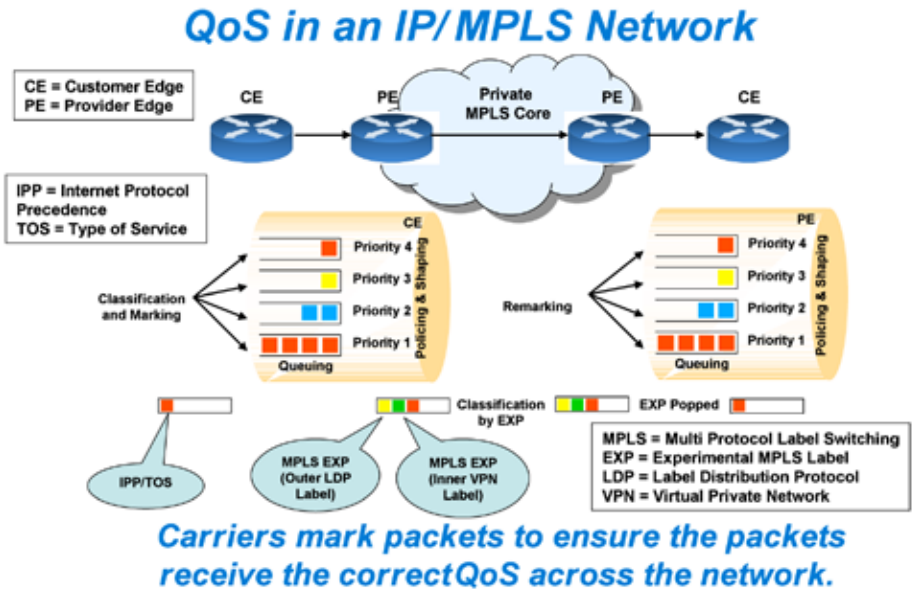


Figure 1

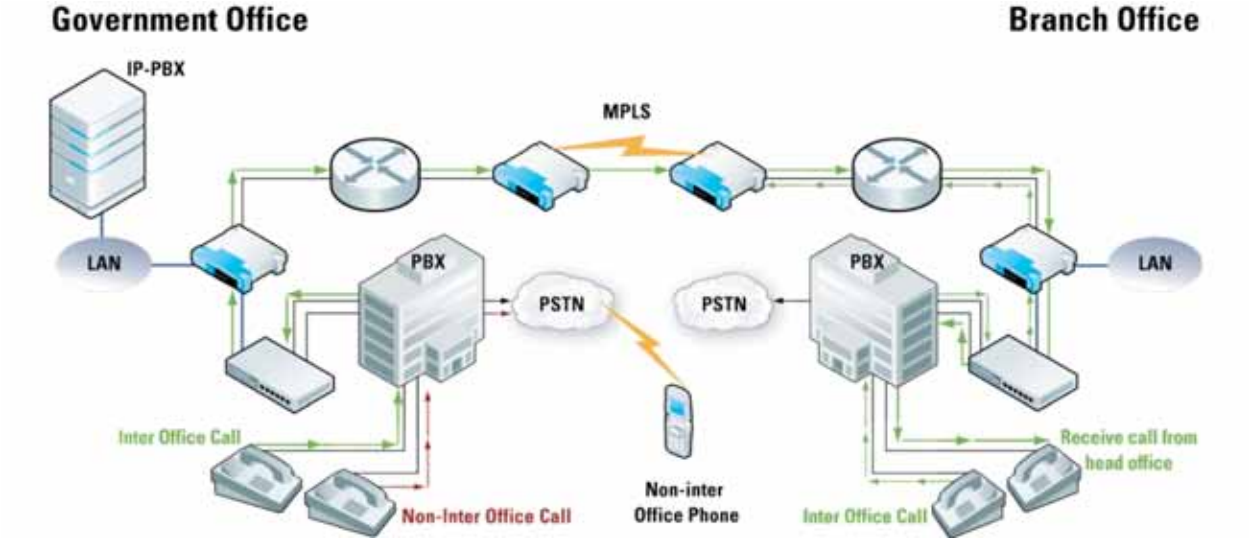


Figure 2

The diagram above depicts how a Government agency office with an IP private exchange (PBX) system can connect with one of its branch offices using MPLS to increase the QoS of the communications path.

Service providers can also use MPLS to ensure national security and emergency preparedness (NS/EP) IP traffic receives the appropriate QoS levels as required by the associated applications.

Ethernet

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). It defines a number of wiring and signaling standards for the physical layer, through means of network access at the media access control (MAC) and data link layer, and a common addressing format. Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. The initial deployment occurred in 1980.

Ethernet is the most-used LAN worldwide. In fact, most data traffic begins or ends on an Ethernet interface. Ethernet allows high bandwidth connectivity, supports multimedia applications, and delivers storage services and server consolidation. The interface speeds on Ethernet have evolved from 10 Mbps to 10 Gbps.

Ethernet technologies allow scalability, traffic engineering, QoS, reliability, and manageability to allow service providers to shape it as an infrastructure for converged, next-generation networks that can better support NS/EP traffic. Ethernet is capable of allowing service providers to deploy native Ethernet services initially, and interwork with MPLS services.

Asynchronous Transfer Mode

Public carriers implement asynchronous transfer mode (ATM) to provide high bandwidth service. ATM is normally deployed in conjunction with a Layer 1 synchronous optical network (SONET) infrastructure. ATM is feature-rich and offers many different services, but other technologies that offer more cost effective capacity and simplified management to integrate voice and video continue to replace ATM. One of the key aspects is its wide support by the American National Standards Institute and International Telecommunication Union for carrying a complete range of user traffic for voice, video, and data for any type of physical media. ATM scalability is limited due to the high cost of chip sets and limited number of implementations that can exceed OC-192 speeds, as IP device requirements are for operation at speeds up to OC-768.

ATM contains QoS capabilities for delivery of real-time traffic and other delay sensitive traffic. QoS is achieved through assignment of traffic to constant bit rate (CBR), variable bit rate, and unspecified bit rate QoS.

For example, ATM CBR allows specification of a QoS to achieve controlled latency, jitter and throughput for real-time applications such as voice or video traffic.

The Internet Engineering Task Force has defined a suite of protocols for carrying IP traffic over ATM, and these standards not only address delivery of best effort traffic, but also standardize the use of RSVP to signal IP application requirements to the ATM infrastructure to allocate QoS resources. Since ATM is still deployed at the edges of many networks, ATM CoS will continue to be used as a means to deliver real-time traffic for the near future. However, the emergence of new technologies such as dense wavelength division multiplexing (DWDM), MPLS and Gigabit Ethernet will more tightly integrate network management and provide higher performance for lower cost than ATM. [25]

Synchronous Optical Networks

Synchronous Optical Networks (SONET) belong to a family of fiber optic transmission rates from 51.84 Mbps (OC-1) to 39.812 Gbps (OC-768) created to provide the flexibility needed to transport many digital signals with different capacities. Moreover, SONET is an optical interface standard that allows inter-working of transmission products from multiple vendors. SONET is widely deployed by carriers, often in a physical ring topology with fast switching between segments or sections (50 milliseconds), with multiple fibers providing transport redundancy. SONET has been widely implemented within carrier domains and has only recently been challenged by DWDM, which, although it lacks robust network management standards, offers higher aggregate speeds and is far less expensive. SONET traditionally has been used to carry time domain multiplexing (TDM) traffic, which is considered not practical for IP traffic due to its high cost; other criticisms of SONET include bandwidth limitations, high overhead and high costs of provisioning. The strongest argument for its continued use in the transport network arena is its strong network management capabilities, a strong set of standards, and the large embedded base of equipment used in carriers' networks.

SONET, in spite of its limitations, has a key role in the next generation telecommunications infrastructure. Carriers have considerable investment in their SONET networks and cannot see enough revenues coming from new services to justify building overlay networks. As a result, SONET will likely not be replaced by an all-optic network or by a native Ethernet transport network within the next ten years. SONET equipment manufactures are evolving their equipment offerings to conform to the carriers' requirements demanding affordable, standards-based platforms that are highly scalable and deliver packet and TDM services both seamlessly and without manual configuration. To achieve these goals, vendors are developing their products to span from the customer core, using advances in multi-protocol traffic adaptation, and developing their products for end-to-end operations management. Industry experts predict that multi-service SONET platforms will be as fundamental to telecommunications networks in the coming decade as routers were to the Internet during the 1990s. [26]

Footnotes

25 See section 2.1.3 of the *NCS Technical Information Bulletin 04-2: Internet Technologies in a Converged Network Environment;* dated December 2004.

26 See section 2.1.4 of the *NCS Technical Information Bulletin 04-2: Internet Technologies in a Converged Network Environment;* dated December 2004.

Congestion

Congestion

A stream of data is separated into packets for transit across an Internet protocol (IP) network. Each IP packet includes both a header that specifies source, destination, and other information about the traffic and the message data itself. Network congestion in the IP network environment occurs when the amount of traffic carried by a link or node exceeds its capacity and results in a deteriorated quality of service level, such as packet delay or loss. [27] With delay insensitive applications, such as e-mail or instant messaging, the effects of packet delay or loss in the IP network will likely go unnoticed by the end user. [28] For delay sensitive applications, such as Voice over Internet Protocol (VoIP), real-time gaming, or IP television, packet delay or loss can affect the application's ability to operate or its quality of the service. Service providers design and manage their networks to avoid or minimize network congestion and to be able to prevent and respond to network events.

The user will only experience performance as good as the slowest link. Congestion can occur in many places along a user's communications path. One cause of congestion can be a mismatch in speed between networks. For example, national security and emergency preparedness (NS/EP) authorized users on a low-speed local area network (LAN) connection, such as a 10 Mbps Ethernet, connecting to servers on high-speed networks, such as a 155 Mpbs asynchronous transfer mode (ATM) over OC-3, may experience congestion at the interface between the networks as the diagram below illustrates. Additionally, if a 10 Mbps connection is supporting hundreds of users within an office, congestion could occur as the users send/receive data due to the size of the connection.

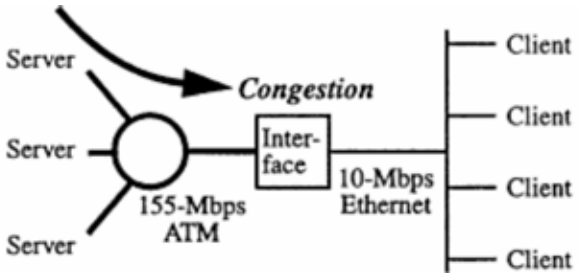


Figure 1 Congestion Due to Speed Mismatch

Congestion can also occur in a network node, such as a router or switch, from traffic aggregation in which traffic from multiple input ports is destined for a single output port. Traffic exceeding the line speed of the output port will be buffered and placed in a queue. Waiting in the queue will add delay to the traffic and overfilling the queue will lead to packet loss and degraded application performance. A congested edge, enterprise, or customer premise router can reduce bandwidth and lead to packet loss. A router placed at the edge of the network to connect various types of users, such as residential, cellular users, satellite communications, or enterprise clients, to the core network may experience congestion at peak traffic times or during network events. At such times, it may not be able to attain the optimum data transfer speeds if a router is congested as packet buffers reach capacity. Congestion in edge routers has the potential to adversely affect the performance of applications that depend on the routers to function effectively. This is also true for the edge router at the receiving end. If a router is receiving, more inquires than it is designed to handle, the users may experience a delayed response. Service providers generally strive to manage capacity on edge router resources so that users do not experience congestion where their traffic enters the network.

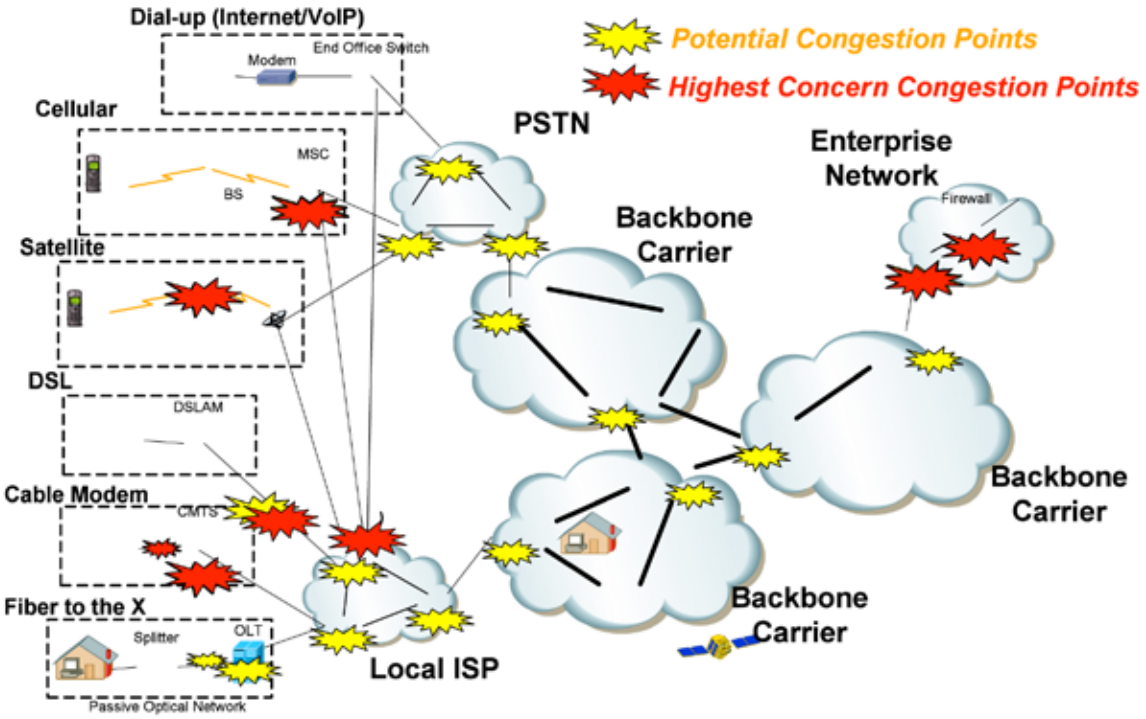


Figure 2 Diagram of Potential Congestion Points

Congestion for digital subscriber line or dial-up customers is generally not at the digital subscriber loop access multiplexer (DSLAM); rather, it is the transport from the Internet service provider (ISP) point of presence to the DSLAM. An inadequate number of ports on the network access server at the ISP can lead to congestion. Further, an overloaded web server could experience congestion during a period of high use. In addition, a user may overload their personal computer with multiple tasks, thus leading to slower service and an ineffectiveness use of an application.

In order to help reduce the possibility of network congestion, a customer can place a fully managed quality of service (QoS) router on its premise. As described in section three, the QoS router has a robust set of QoS mechanisms it can employ to identify voice traffic (inbound or outbound) and ensure that the required amount of bandwidth is made available. Additionally, a highly reliable and simple to implement approach to reduce the possibility of network congestion is to provision a dedicated connection from the customer premises to the IP network edge with bandwidth sufficient to preclude any potential congestion.

Footnotes

27 Use of the term congestion should not be construed to mean a stoppage of data flow; rather it is a delay in the delivery of packets until sufficient network capacity is available to carry them to a device or application.

28 With these types of services, data can be sent on a store and forward basis, meaning that the data is sent when the transmission path is available. Since the action is not real time, the receiver is unaware of the delay.

Network Management

Network Management

Network management is a key requirement for successful operations in both the circuit switched and packet switched network environment. Network management techniques evolve as network technology advances, including the ability to manage traffic within and across Internet protocol- (IP) based network overlays. While managing networks, providers monitor traffic flow and performance to optimize data flow across the network for all users. Network management for IP networks includes monitoring the network for service failures or down ports; service degradation including packet delay/loss and jitter; traffic anomalies, such as border gateway protocol routing; and congestion conditions. For circuit-switched voice communications, network management involves responding to incidents such as during an unusual mass calling event or congestion caused by reduced capacity due to out-of-service conditions, such as trunk failure.

To control the traffic, network managers generally have two categories of mechanisms:

- **Expansive controls** temporarily expand the available capacity and successfully complete customer service via alternate paths. A simple example is moving service onto a preprovisioned protection path, which exists in the network solely for the purpose of service protection in the event of the loss of a primary path. More complex examples involve rerouting circuit switched voice calls through alternate routes, or adjusting the flow parameters of IP traffic, to redirect traffic away from a congested path and onto paths that have capacity available to handle the extra load.

- **Protective controls** stop traffic that cause network harm due to volume-related congestion, such as radio call-in promotions when call volumes traditionally increase or during an intentional distributed denial-of-service (DDOS) attack. Filtering and eliminating malicious traffic associated with cyber attacks or canceling traffic to a destination that is known to be out of service so that it does not consume unnecessary capacity are examples of a protective control response.

The terrorist attacks of September 11, 2001, in New York City provided an example of the importance of managing traffic to avoid network congestion. This attacks resulted in increased network traffic as people attempted to locate each other, in some cases between 150 and 400 percent of the normal calling volume, with most of it concentrated toward lower Manhattan. Carriers recognized that the attack had destroyed some business offices and their associated communications equipment. Rather than transporting traffic destined for the impacted area from another location and consuming network capacity, carriers blocked voice traffic at its origination, keeping resources available to transport other traffic with a higher probability of completion. Other examples of network congestion events include holidays that cause a high volume of traffic, mass calling events, bad weather, or cyber attacks.

The three basic key enablers of traffic management on the Internet consist of the IP addressing concept, routing protocols, and the physical infrastructure of routers and connectivity that provides the communications pathway. Specifically:

- IP addressing allows the unique identification of any device connected to the public Internet. The addresses are associated with specific ports on physical networks. Each service provider manages the assignment of one or more continuous ranges of IP address. The structure of the address allows fast identification of the network, or autonomous system, to which any device is currently connected. In effect, the service provider assigns each active device a unique IP address, which is associated with a specific port, or physical termination, within the service provider's network.

- Routing protocols allow one network to exchange information with another network. When a packet is received, the destination address is compared to the information in the routing table. The packet is then passed to the next router, which advances the packet to its ultimate destination at the lowest cost. This means that information moves across an

IP network, like the Internet, by hopping from one router to the next with each hop moving it closer to its destination. This allows billions of devices to connect users without the need for each individual network and device to have a predefined path to its destination.

- The ability for two devices to communicate also requires Internet service providers (ISP) to establish a physical connection, which consists of either fiber or copper cables, to buildings and equipment. The ISPs deploy the routers that analyze the IP addresses associated with each packet and invest in the facilities connecting routers to each other and to the end users.

Acronym List

Acronym List [29]

ATM	Asynchronous Transfer Mode
CBR	Constant Bit Rate
DHS	Department of Homeland Security
DSLAM	Digital Subscriber Loop Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing
FCC	Federal Communications Commission
GETS	Government Emergency Telecommunications Service
IP	Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
MPLS	Multi Protocol Label Switching
NCS	National Communications System
NGN	Next Generation Network
NS/EP	National Security and Emergency Preparedness (NS/EP)
NSTAC	President's National Security Telecommunications Advisory Committee
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
SONET	Synchronous Optical Network
QoS	Quality of Service
SLA	Service Level Agreement
TDM	Time-Division Multiplexing
TSP	Telecommunications Service Priority
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WPS	Wireless Priority Service
X.25	An ITU-T standard network layer protocol

Footnote

29 *Newton's Telecom Dictionary 22nd Edition* used for Terms.

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on the Physical Assurance of the Core Network

November 6, 2008

For information on this report, please contact the

National Communications System
nstac1@dhs.gov

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Response to the Sixty-Day Cyber Study Group

March 12, 2009

For information on this report, please contact the

National Communications System
nstac1@dhs.gov

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Cybersecurity Collaboration

Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability

May 21, 2009

Table of Contents

Executive Summary

At the direction of the Executive Office of the President and following a comprehensive scoping effort, the President's National Security Telecommunications Advisory Committee (NSTAC) established the Cybersecurity Collaboration Task Force in November 2008 to explore the need for and feasibility of creating a joint 24/7 public-private operational capability focused on improving the Nation's ability to detect, prevent, mitigate, and respond to significant cyber incidents.

Protecting the United States' (U.S.) cyber and underlying critical infrastructures is essential to the Nation's homeland and national security, public health and safety, economic vitality, and way of life. Today's global economy, military operations, and public-private sector endeavors depend on the ability to operate in cyberspace. Meanwhile, the magnitude, nature, and sophistication of cyber threats pose increasingly greater consequences, highlighting an urgent need for protective action. Critical infrastructures such as banking and finance, communications, energy, information technology, and transportation are interdependent, with disruption of one having the potential to dramatically affect the others. As a result of these dependencies and interdependencies, the Nation's ability to operate with complete effectiveness in cyberspace is at serious risk. At the same time, the lines of responsibility between the public sector and the private sector for addressing cybersecurity and interdependency issues are blurred. Consequently, an urgent need exists for an overarching operational framework for coordination and response that more fully integrates the public and private sectors' efforts in this area. Development of a framework that can fully and strategically address the cyber threat must be a matter of national priority.

The Task Force's primary finding is that the integrated, operational information sharing and cyber response mechanisms needed to adequately address the cyber threat do not exist today. Given the threat environment, and the global reliance upon cyber technologies and networks, a national capability to prevent, detect, mitigate, and respond to cyber incidents of national consequence in a timely, effective manner is critical to national security. Although a variety of strategic, policy, and legal issues are associated with our Nation's ability to safely and effectively operate in cyberspace, the most significant gap is the lack of an operational mechanism for the Government and private sector to collaborate and coordinate during cyber events.

Based on the authorities and responsibilities established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* the NSTAC recommends to the President to direct the establishment of a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability to address cyber incidents of national consequence.

This recommendation proposes establishing a Government-sponsored Joint Coordinating Center (JCC) for public and private sector representatives from various critical infrastructures and key resources sectors following the aggressive, phased approach described in the report. Specifically, the JCC would initially build upon the current coordination/collaboration capabilities of the National Coordinating Center and the U.S. Computer Emergency Readiness Team, and incorporate other existing cyber incident monitoring and response public-private entities. The JCC capability should be located in a Government facility with around-the-clock operations and supporting tools and collaboration capabilities. The JCC's primary mission would focus on robust information-sharing for developing and sharing cyber situational awareness, and would institutionalize the time-sensitive processes and procedures to detect, prevent, mitigate, and respond to cyber incidents of national consequence.

1 Introduction

1.1 Purpose

For many years, the President's National Security Telecommunications Advisory Committee (NSTAC) has recognized that, in today's converged environment, cyberspace is a strategic asset and protecting the Internet's integrity and availability is a national security priority. [1] In this report, the NSTAC examines national security and emergency preparedness (NS/EP) communications issues in a converged environment and provides recommendations to help ensure the Internet's integrity and availability now and in the future.

DPMR Capability

Detection: Developing an understanding of normal network traffic volume and flow using independent sources will help the JCC participants detect anomalies. Stakeholders will work with partners to obtain external data on threats and vulnerabilities.

Prevention: Developing proper interdiction guidance for prevention activities. Prevention activities include bi-directional information sharing within the IT and communications sectors, and with government (Federal, State, and local) and international agencies.

Mitigation: Developing the mitigation tools and technology will help stakeholders to address cyber incidents, while ensuring stability within other unaffected networks.

Response: Organizing teams, processes, and procedures will help stakeholders to coordinate internal and external sources to respond to and recover from incidents.

This report outlines the United States' (U.S.) need to develop a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response (DPMR) capability. [2] The cyber incident DPMR capability—the Joint Coordinating Center (JCC)—will consist of operational coordination and liaison functions, with the physical or virtual participation of the private sector critical infrastructure and key resources (CIKR) community. The capability is necessary to enable the Nation to defend itself from threats and vulnerabilities that jeopardize its ability to rely on cyber space. In addition, this operational capability will be a focal point for developing, monitoring, and creating a common situational awareness of threats and vulnerabilities in general and the operational impact of cyber incidents of national consequence in particular. Where feasible, the JCC would collect warning and threat information to enhance preparedness of both public and private sector cyber stakeholders through fostered collaboration and unity of effort. This may also include recommendations for protective measures or mitigations.

This report underscores the importance of creating a cyber incident DPMR capability. The single most critical improvement to the protection of both public and private sector cyber-based systems is the routine communication about new or evolving threats and vulnerabilities (sometimes referred to as 'indications and warnings') among all key stakeholders responsible for protecting cyber networks and systems. In this report, the NSTAC presents a framework for initiating this comprehensive cybersecurity operational capability, identifies and analyzes policy considerations that may affect future capabilities, outlines parameters for the envisioned end state, and offers recommendations for phased implementation.

1.2 Background/Need

The reflection upon my situation and that of this army produces many an uneasy hour when all around me are wrapped in sleep. Few people know the predicament we are in.

~ General George Washington, 1776

Today, an adequate national operational capability to respond to the current growing cyber threat does not exist.

Over the last 20 years, the Nation has become increasingly dependent on information technology (IT), interacting and communicating seamlessly across vast networks traversing the globe. This reliance on interconnected IT systems also exposes the Nation to significant cyber threats and vulnerabilities, placing our CIKR [3] at risk. Today, an adequate national operational capability to respond to the current growing cyber threat does not exist. Cybersecurity issues have been addressed piecemeal in varying

ways by different government entities at the Federal, State, local, tribal, and territorial level; private companies and industry organizations; and academic institutions. Although these groups have initiated and sustained various levels of collaboration, cyber threat and vulnerability concerns require an even more systematic, integrated approach. [4] Recognizing the growing interdependencies between cybersecurity and CIKR, these groups are addressing cybersecurity from a national security perspective, rather than from a merely technology perspective. However, these efforts are works in progress; the need for an increasingly collaborative and systematic approach remains.

CIKR Interdependencies and Threat Actors

The Nation's ability to function as a global leader depends on a variety of critical infrastructures and cyber technologies that enable the economy to operate within the global marketplace. For example, increased consumer access to electronic commerce has changed the face of the marketplace; migration to electronic medical records will improve the quality of healthcare; and power distribution systems are moving to a 'smart grid' delivery concept, which is highly dependent on cyber technologies. This critical reliance on cyber and communications networks is intensified by a growing interdependence among these networks and other CIKR.

Such interdependence was demonstrated and highly visible during the August 2003 Northeast blackout. Immediately before the blackout, a computer worm disrupted an Ohio power plant's indications and warnings system, degrading its ability to receive critical data regarding the health of the power plant and grid. Although the worm did not directly cause the blackout, it created confusion and prevented the plant owners and operators from receiving warnings that would have alerted them to the failures in the grid so they could have taken measures to protect the power plant. This failure within the energy sector disrupted cyber and communications networks throughout the Northeastern United States and areas in Canada, underscoring the interdependencies between cyberspace and other CIKR sectors. [5] Potential adversaries have undoubtedly noticed these vulnerabilities and the United States' disjointed incident response.

> Various entities have carried out cyber attacks against cyber systems and underlying infrastructures.

In addition to these growing interdependencies, the United States has witnessed the rise of a diverse and aggressive range of threat actors and various entities carrying out cyber attacks against cyber systems and underlying infrastructures. These threat actors include: agents of nation-states, lone wolf hackers, cybercrime organizations, and terrorists, among others. These malicious actors are relentlessly exploiting the complexity of the interconnected environment and the anonymity of the Internet to access communications and data networks, presenting new risks to U.S. cyber and national security. Future concerted cyber attacks against U.S. national infrastructures could be severe or catastrophic.

> Future concerted cyber attack against U.S. national infrastructures could be severe or catastrophic.

These looming threats came to fruition in incidents such as the 2007 cyber attacks against Estonia, the 2008 cyber attacks against Georgia, and the 2008 cyber attacks against the Department of Defense (DoD). In 2008, the World Bank suffered a series of Internet attacks that penetrated at least 18, and perhaps as many as 40, of the bank's data servers. In March 2009, the *New York Times* reported on a world-wide cyber espionage network known as GhostNet. This network targeted organizations and individuals in 103 countries and used malicious software to steal sensitive information. [6]

Most recently, since November 2008, malicious code known as Conficker spread to more than 12 million computers worldwide. In response to this threat, a number of private sector and government representatives informally joined together to form the Conficker Working Group to develop mitigation techniques to respond to the evolving threat. The working group conducted its activities in an ad hoc and self-organizing manner, and was instrumental in reducing the impact and infection rate of U.S. computers. [7] However, Conficker continues to pose

challenges and risks for the global Internet community. The depth and breadth of Conficker's spread highlights the value of public-private sector cybersecurity collaboration and how a joint, integrated capability would more likely offer an established and secure place to coordinate these kinds of efforts.

International geopolitical events, such as the cyber attacks against Estonia and Georgia, demonstrate that the Federal Government would benefit from immediate, expert, and authoritative private sector involvement in response to such events. Public-private cooperation provides a valuable mechanism for subject matter experts to contribute to protecting America's cyber infrastructure.

Beyond their susceptibility to cyber-specific threats, the complex interdependencies of the various infrastructures, cyber and communications networks are also subject to the threat of natural disasters (for example, hurricanes, floods, earthquakes, and wildfires) and physical events (for example, train derailments, undersea cable cuts, and bombs), as documented in the NSTAC's *2006 Global Infrastructure Resiliency (GIR) Report.*[8] The threat of natural disasters and disruptive physical events can significantly impact the cyber environment with long term effects. In addition to being vulnerable to physical and cyber threats, these networks are also vulnerable to electromagnetic pulse attacks.[9]

The threat of natural disasters and disruptive physical events, such as cable cuts or train derailments, can significantly impact the cyber environment with long term effects.

Disruptive events in any of these areas can significantly impact the cyber environment with long-term effects. Consequently, current DPMR activities associated with the physical protection and restoration of CIKR cannot be subordinated to cyber response. Rather, physical and cyber DPMR activities must be approached in conjunction with each other, and cannot be treated as separate processes or functions.

The Need for an Operational Solution

Government and private sector subject matter experts recognize the urgent need for and value of a public-private sector collaborative DPMR capability.

There is no operational mechanism across all sectors for a coordinated and unified effort to detect, prevent, mitigate, and carry out a real-time response to significant cyber issues affecting the Nation. Government and private sector subject matter experts recognize the urgent need for and value of a public-private sector collaborative DPMR capability. Previous reports, such as the 2003 President's *National Strategy to Secure Cyberspace,*[10] the Department of Homeland Security (DHS) *2007 Tiger Team Report*[11] and the 2006 NSTAC *Next Generation Networks Task Force Report,* recommended establishing a joint coordination center where the public and private sectors could share cybersecurity information. The NSTAC issued the following recommendation:

> *A joint coordination center for industry and Government should be established. This would be a cross-sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies. Such a center would improve communications between industry and Government as well as among industry members, and would incorporate and be modeled on the NCC.*
>
> *The center should be a Government-funded, appropriately equipped facility, manned jointly by experts from all key sectors. In a fully converged (Next Generation Network [NGN]) environment, everything will be interconnected and interdependent to a greater degree, and thus means of coordinating among all key sectors must exist. Physically collocated, joint manning is vital to achieve the high level of interpersonal trust needed for sharing sensitive specific information and to achieve the level of mutual credibility required in a fast-paced decision-oriented environment. It should provide the full set of planning, collaboration,*

and decision-making tools for those experts to work, whether together as a whole or in focused subgroups. [12]

Previous reports recommended establishing a joint coordination center where the public and private sectors could share cybersecurity information.

The proposed cyber incident DPMR operational capability is envisioned to address disruptions and attacks to national CIKR that occur via the U.S. cyber infrastructure. [13] A variety of entities currently have defined and limited responsibilities; there is no overall entity responsible for cross sector coordination and response during time-critical cyber incidents of national consequence. The National Coordinating Center (NCC) has coordinated a variety of activities between the Federal Government and the private sector for more than 25 years. Although the NCC's charter does not preclude coordinating cyber incidents, it has historically focused on issues associated with the physical side of the Nation's telecommunication infrastructure. Information sharing within the Network Security Information Exchanges (NSIE) focuses on cyber vulnerabilities and threats, but does not focus on immediate, operational activities. The U.S. Computer Emergency Readiness Team (US-CERT) is charged to provide outreach to the private sector, but could benefit by broadening its interaction with NCC Industry Members and other private sector participants. There are other examples of joint private-public collaboration, primarily in the post-incident cyber domain. However, these are not focused on early indications and warnings, but rather on post-incident investigations, some of which have law enforcement aspects. In addition, organizations have made little progress in assessing the threat environment and aligning cyber incident management efforts. In short, despite the existence of a number of coordination mechanisms and capabilities, there is currently no overarching, integrated public-private, 24/7 operational cyber incident DPMR capability.

Many factors have contributed to this situation, such as shifting priorities, budget constraints, and the blurred lines of ownership and jurisdiction over these issues. These factors affect both the Government and the private sector. Nonetheless, the NSTAC believes a critical first step in implementing some of these recommendations is establishing an initial operational capability that allows all appropriate players to share information, establish a baseline understanding of the threats to our Nation's critical infrastructures, and take action to detect, prevent, mitigate, and respond to cyber threats.

An urgent and growing need exists to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors.

Since 1991, the NSTAC has recommended creating a cyber collaboration capability, and recognizes progress such as the creation of the IT and Communications Sector and Government Coordination Councils. [14] Although these achievements have improved cybersecurity collaboration, the NSTAC believes that operational collaboration and coordination between the Federal Government and private sector must improve. An urgent and growing need exists to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors.

The NSTAC has further recommended to the Government that the private sector should be elevated to the status of a trusted partner, and that the public and private sectors should share critical and time-sensitive threat information to strengthen the threat and warning architecture. [15] The Federal Government has the tools and abilities to gather information on the capabilities and intentions of adversaries in cyberspace, but does not adequately share this data with the private sector. Without jeopardizing its sources and methods, the Government must share this data with the private sector, including information regarding planned attacks and the assets that may be in danger. This advanced information will give the infrastructure owners and operators more time to take protective measures to deflect attacks or minimize their impact. Such measures can limit negative effects both on the private sector and its immediate customers, as well as the extended, interdependent CIKR. [16]

Elevating the private sector to trusted partner status is the foundation for any future collaboration effort, and is a policy decision that should be made and supported at the highest levels of Government. The Federal Government and the private sector should improve their awareness of shared risk, consequences, dependencies, and cascade effects; they must also clarify decision-making authority and their respective response and reconstitution roles. The desired outcome of these improvements is clear guidance and an enhanced ability to rapidly execute national-level decisions for response options to sophisticated attacks against our shared information infrastructure. [17] This outcome can only be accomplished by first acknowledging that the risk associated with partnering with the private sector outweighs the consequence of not doing so.

1.3 Charge

At the request of the Executive Office of the President (EOP) to examine the issue of cybersecurity collaboration, NSTAC established the Cybersecurity Collaboration Task Force (CCTF) in November 2008 to explore the need for and feasibility of creating a joint public-private, 24/7 operational cybersecurity collaborative DPMR capability. The CCTF also examined the opportunities and challenges to developing this cyber incident DPMR capability.

The report examines the feasibility of developing a new cyber incident DPMR capability or expanding the operational focus of existing cyber watch functions, and identifies the issues that may impede or preclude achieving this objective. Moreover, the report also proposes recommendations for resolving these issues.

1.4 Process

The CCTF identified issues that may affect the development and deployment of a cyber incident DPMR capability, including trust issues between the public and private sectors and policy considerations. Section 3.0 describes these issues.

The Task Force conducted a gap analysis of existing collaboration models and capabilities to determine mechanisms that may be developed or enhanced to establish a national cyber incident DPMR capability. The data-gathering included interviews with subject matter experts and internal discussions among Task Force members. Based on its findings, the Task Force then developed recommendations.

During interviews with the CCTF, key public and private sector subject matter experts identified existing operational capabilities that may serve as a basis for a cyber incident DPMR capability. [18] The CCTF posed the following questions to all presenters regarding public-private cyber incident DPMR capabilities:

- Can the capabilities be provided under the current contractual, legal, and regulatory framework? If not, what would need to change to support any given capability?
- Are the capabilities currently technically feasible? If not, what would be necessary to move in that direction?
- Assuming the desired capabilities are lawfully and technically feasible, what operational and/or business model would best suit participation by the private sector CIKR in this initiative?
- What cultural/trust issues must be addressed?

2 Desired End State: 24/7 Cyber Incident DPMR Capability

2.1 Joint Coordinating Center (JCC)

To achieve the desired end state of a joint, integrated public-private, 24/7 operational cyber incident DPMR capability, the NSTAC recommends that, under the direction of a Federal department or agency identified by the President, members from both the public and private sectors build upon current NCC and US-CERT capabilities and integration efforts and extend these capabilities to develop a JCC capability. The principal feature of the JCC is rich, timely, bi-directional sharing of information between the public and private sectors that ensures their ability to detect, protect, mitigate, and respond to cyber threats.

The principal feature of the JCC is rich, timely, bi-directional sharing of information between the public and private sectors that ensures their ability to detect, protect, mitigate, and respond to cyber threats.

Governance – Clarity of Mission, Roles, and Responsibilities

There is a lack of clear authority and budget responsibility for a public-private cyber collaboration capability; cyber collaboration capabilities currently exist, but are largely uncoordinated.

To achieve success and maximum value, the proposed JCC capability requires clearly defined authorities, oversight, management, responsibilities, roles, and resources. There is a lack of clear authority and budget responsibility for a public-private cyber collaboration capability; cyber collaboration capabilities currently exist, but are largely uncoordinated. In addition to approving this JCC capability, the NSTAC recommends that the President should:

- Designate the Executive Branch organizations that will participate as members of the JCC and contribute personnel and other resources;
- Designate a lead organization or sponsor; and
- Direct budget and authority provisions to properly implement, operate, maintain, and evolve the proposed JCC capability.

The lead organization or sponsor should convene a working group, leveraging the membership and expertise of existing organizations such as NSTAC member companies and members from appropriate Government and Sector Coordinating Councils, and task the working group to develop the initial concept of operations (CONOPS) to govern the JCC. The CONOPS will refine the JCC's:

- Mission and purpose;
- Membership requirements and eligibility;
- Designated leadership (to consider private sector co-chairs);
- Desired operational capabilities and coordination and liaison functions;
- Governance structure; and
- Other details necessary for its establishment.

The CONOPS will identify actions required to implement the JCC. The NSTAC understands that Phase I activities will be the most urgent, specific, and immediately actionable tasks.

Given this matter's sense of urgency and its link to national, homeland, and economic security, it is imperative to establish an achievable but aggressive timeline to execute an implementation plan for the JCC. The NSTAC recommends that the working group complete the CONOPS and launch the JCC soon thereafter. [19] Upon approval, the JCC would be implemented through a phased approach, as described in Sections 2.2 and 2.3. A phased implementation approach will allow enhanced capabilities to be established in an affordable and efficient manner. The NSTAC offers an implementation timetable for consideration in Appendix B.

A phased implementation approach will allow enhanced capabilities to be established in an affordable and efficient manner.

The NSTAC recommends that the JCC be housed in a Government-funded and appropriately equipped facility. The facility should be based in the Washington, DC, area to leverage the expertise and existing collaboration centers located in this region; however, NSTAC believes that a back-up facility should be based in another part of the United States to provide resiliency and ensure continuity of operations. In a fully converged, networked environment, JCC functions would be interconnected and interdependent to a greater degree, enabling all key sectors to coordinate with each other. [20] In turn, representatives from all key sectors will jointly operate the JCC. In some

cases, representatives will be physically collocated; in other cases, they will be virtually connected. Physical collocation and joint operations are vital elements to achieve the interpersonal trust and level of mutual credibility required for sharing sensitive, detailed information in a fast-paced, decision-driven environment. [21] In addition, there is a need for controlled communications mechanisms to enable sharing information among all those authorized to access the information. [22]

Finally, the NSTAC notes that these recommendations are consistent with the objectives and recommendations of the President's Comprehensive National Cybersecurity Initiative (CNCI). Although Initiative #5 focuses on linking certain Federal cyber operations centers to improve cyber threat awareness and incident response actions, it focuses exclusively on the U.S. Government. Some of these centers are also critical components in our recommended joint public-private sector capability. Initiative #12 recommended expanding the joint operational capability of the US-CERT and the NCC to include private sector CIKR sector participation, to eventually incorporate voluntary participation from all 18 CIKR sectors.

2.2 Operations

Successful models of public-private sector collaboration currently exist in practice, such as the long history of the NCC for communications-related matters. The NCC model operates within the existing legal and policy frameworks, and should be leveraged as an integral element for future public-private cyber security collaboration. Leveraging both the NCC and the US-CERT, as well as other capabilities, a fully-developed JCC capability can allow public and private sector representatives to share information, which will improve cyber incident DPMR. The JCC will have a 24/7 watch and warning capability, with surge capacity during emergencies. To expedite the implementation of this capability, the NSTAC recommends a phased approach.

Successful models of public-private sector collaboration currently exist in practice, such as the long history of the NCC for communications-related matters. The NCC model operates within the existing legal and policy frameworks, and should be leveraged as an integral element for future public-private cyber security collaboration.

The first phase will leverage existing collaboration models within the public and private sectors and establish a foundation for extending collaboration capabilities. The key elements associated with the first phase are:

- Extending the current presence of communications company representatives to the physical/virtual presence of Information Sharing and Analysis Center (ISAC) representation from the communications, financial services, IT, and power sectors;
- Establishing the baseline information needs of both private sector and Government partners;
- Creating an initial CONOPS predicated on those baseline information needs; and
- Testing that CONOPS for a period of time to ensure that the approach is sound.

Follow-on phases will improve on these existing models and develop more robust information sharing to achieve enhanced cyber incident DPMR capabilities. These phases would include expansion of U.S. Governmental and international participation, extended private sector participation, and enhanced training and exercise support.

Appendix B provides a phased-approach implementation of the JCC. The table suggests an aggressive implementation timeline commensurate with the urgency of addressing this need. The complexities of this effort require sustained high-level attention to ensure success.

Table 1 – Core Phase I JCC Membership	
Federal Government	▶ Department of Homeland Security • US-CERT • NCC Watch • National Cyber Security Center (NCSC) ▶ Department of Defense • Joint Task Force Global Network Operations' (JTF-GNO) Security Center • Defense Cyber Crimes Center (DC3) ▶ Department of Justice's National Cyber Investigative Joint Task Force (NCIJTF) within the Federal Bureau of Investigation (FBI) ▶ Federal Communications Commission (FCC) ▶ Department of Commerce
Private Sector	▶ Carriers ▶ Internet Service Providers (ISP) ▶ Security companies ▶ Content providers ▶ Hardware/software vendors ▶ Owners/operators representatives ▶ Representatives from the Banking and Finance, Communications, Electric, and IT ISACs
International Community	▶ Key allies, such as • Australia • Canada • New Zealand • United Kingdom ▶ Other international organizations, such as • Forum of Incident Response and Security Teams • International Watch and Warning Network, • North Atlantic Treaty Organization • Interpol

2.3 Membership

Planning and execution of national cyber detection, prevention, mitigation, and response capabilities requires joint participation of many domestic public and private sector organizations, in addition to international entities.

Planning and executing national cyber incident DPMR capabilities requires joint participation of many domestic public and private sector organizations, in addition to international entities. Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities. Combining all stakeholders into a single Government-funded/equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution.

Although the CONOPS will outline longer-term membership requirements, core Phase I JCC membership should include, but not be limited to, the U.S. Government, the private sector, and the international community. Examples are provided in the Table 1.

Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities.

The NSTAC notes that work is currently underway to better align the Government's own operational centers for better situational awareness, through the CNCI. Listing the Government centers above is not meant to interfere with the Government's own organizational activities. Rather, by naming these centers, we are acknowledging that their capabilities may be critical components in our recommended joint public-private sector capability, and making known our desire to coordinate and collaborate with those capabilities.

During the JCC's subsequent development phases, additional cybersecurity-focused departments, agencies, and private sector groups may participate to improve the depth of information sharing. These groups could provide additional subject matter expertise and operational experience to further the JCC's capabilities. Such members could include:

- Other ISACs;
- Intelligence Community Incident Response Center (IC-IRC);
- National Security Agency Threat Operations Center (NTOC);
- SANS Internet Storm Center (ISC);
- National Cyber-Forensics Training Alliance;
- North American Network Operators Group; and
- Carnegie Mellon University's Computer Emergency Response Team Coordination Center.

Combining all stakeholders into a single Government-funded and equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution.

For security purposes, all members should be required to hold a clearance at a level to be determined in the CONOPS. In addition, the CONOPS will identify any special security clearance considerations for the core members (including international partners) to facilitate their participation in a secure environment.

The NSTAC recommends that a mechanism for rapidly and effectively coordinating among all key sectors be established to address security needs in the new cyber environment. Incident response, including response planning, requires a joint public-private sector effort to improve coordination and establish an inclusive, comprehensive, and effective response capability. [23]

2.4 Information Sharing to Enable Operational Collaboration

The JCC's core function is operational collaboration enabled by strong, effective information sharing, which is vital in a cyber threat environment that is relentless and increasing in scope. The JCC's success depends on the extent to which public and private sector members acquire, use, share, and act upon information. This sharing must be bi-directional and timely. The U.S. Government and the private sector must establish mechanisms to protect sensitive information (e.g., proprietary information, personal information, and intellectual property) and to address antitrust concerns.

In an effort to design a robust, effective, and legally-protected information sharing environment for the proposed cyber incident DPMR capability, the NSTAC examined a number of considerations, specifically:

- Cultural/trust and technological considerations; and
- Legal, regulatory, and international considerations.

The cultural and technological considerations are addressed below; the regulatory, legal, and international considerations are addressed in Section 3.0.

Cultural/Trust Considerations

Cultural challenges arise in creating a cyber incident DPMR capability because the Government and the private sector have different organizational objectives, which may conflict with coordinated, integrated, and

seamless information sharing. The Government's mission focuses primarily on protecting the Nation's security; the private sector focuses on serving and protecting its customers. These objectives themselves may not be mutually exclusive, but they can result in incompatible information sharing practices. Consequently, the Government and the private sector must examine and overcome such difficulties and reach common ground to productively share cybersecurity data.

As a result of a lack of guidance and clarity regarding these considerations, the private sector has been reluctant to offer the Government cybersecurity data relating to critical infrastructure. A long-term approach to overcoming these barriers and alleviating liability concerns is to develop a protected and legally acceptable process to secure, use, and share cybersecurity data with the Government, without jeopardizing the privacy of the private sector and its customers.

Another concern is the issue of mutual trust between the Government and the private sector. For instance, the Intelligence Community (IC) currently classifies information to protect the sources and methods of its intelligence collection activities. The IC is therefore reluctant to share detailed cybersecurity threat data, fearing that the private sector may not adequately protect the sources of this information. Exposure of classified data could clearly hamper the IC's ability to effectively gather further information, but failing to share threat data with the private sector could also lead to a distorted or incomplete view of the common operating environment. The IC's reluctance to share cybersecurity threat data exacerbates the trust issue between the Government and private sector.

To ameliorate this problem, the Government and the private sector can gradually establish mutual trust by working closely together on their common goal to detect, prevent, mitigate, and respond to future cyber attacks. For example, the Government can develop tearline procedures to protect the IC's classified sources and methods, and still provide sufficient information about the threat itself to allow the private sector to take mitigation measures. [24] This early, advance information will give the infrastructure owners and operators more time to take protective measures to deflect attacks or minimize their impact.

Technical Considerations

> Tools, techniques, methods, and procedures must anticipate and keep pace with a rapidly evolving threat.

The JCC will require tools for monitoring cyber infrastructure data, developing situational awareness, and coordinating response activities among all key sectors. In a collocated environment with a virtual collaboration capability, experts will need the best supporting tools to successfully prevent and manage the evolving attacks. The most significant threats are the attacks that have not yet been predicted by security experts, such as those involving innovative strategies and techniques. The increased speed and scope of attacks, and the complexity of coordinating remediation efforts, exceed human capacity for manual analysis and response in a timely and effective manner. Tools, techniques, methods, and procedures must anticipate and keep pace with a rapidly evolving threat. Investment in research and development will produce tools to support advanced cyber incident DPMR activities.

> The JCC requires a robust, resilient and secure communications system with the critical infrastructure and key resources owners and operators to facilitate the cyber incident detection, prevention, mitigation and response capability.

Another technical challenge to establishing a cyber incident DPMR capability is secure communications. The JCC requires a robust, resilient and secure communications system with the CIKR owners and operators to facilitate the cyber incident detection, prevention, mitigation and response capability. Such a communications system will allow Government and private sector participants (both physical and virtual) to communicate and coordinate if the JCC primary communications system is disrupted. Additionally, using robust logging and encryption technologies

to protect the confidentiality and the integrity of the communications is essential to prevent adversaries from intercepting the JCC participants' cyber incident response communications. The NSTAC recommends that the JCC cyber incident DPMR capability include a redundant and secure communications system to facilitate public-private collaboration.

3 Legal Considerations

The successful creation and execution of the JCC mission requires public-private sector information sharing, which raises legal, liability, antitrust, and privacy issues for all parties involved. Phase I of the JCC capability is predicated on sharing information to the extent feasible in today's legal environment. However, to move beyond the immediate capabilities and achieve the end-state envisioned for the JCC, the Task Force evaluated aspects of the current legal environment – including regulatory issues, case law, and contractual provisions – that must be addressed to expand information sharing capabilities in the JCC context.

3.1 Current Legal Environment

In its 2003 *Legislative and Regulatory Task Force Report,* the NSTAC analyzed legislative and other impediments to information sharing. [25] Although the information sharing environment has evolved since then, legal provisions regulate information acquisition, use, and sharing.

With respect to antitrust issues, the proposed 24/7 JCC envisions the participation and collaboration of private sector competitors across a number of sectors. Collaboration among competitors raises antitrust concerns, warranting a review of antitrust legislation. The *Sherman Antitrust Act of 1890* [26] precludes any collective activity that has the probable effect of lessening competition in the marketplace. [27] Because the NCC model currently operates within the existing legal and policy frameworks, the NCC framework offers a relevant template to use to initiate the Phase I capability, and should be leveraged for future public-private sector cybersecurity collaboration. To eliminate any ambiguity, the NSTAC recommends that an antitrust review be conducted to include activities planned in the second and later phases of the JCC's development.

Several complex statutory provisions *may* impact the ability of all interested parties to acquire, use, and share information relevant to cybersecurity threats. While not a comprehensive list, the laws listed below set the parameters for cybersecurity collaboration and could limit near real-time, public-private, operational cybersecurity collaboration. [28] Table 2 depicts the law that applies to content in both real-time interception and in stored communications.

- The *Wiretap Act* (1968) broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. Although some statutory exemptions arguably allow cybersecurity initiatives, privacy advocates and others may disagree with some of the applications of these exceptions to cybersecurity activities, which may create uncertainty that could discourage parties from comprehensive information sharing related to

Table 2 - Incident Response: Monitoring Communications During an Incident 29

Timeliness of Information Accessed	Access to Communications Content	Access to Communications Metadats (Headers, Logs, and Other Information)
Real-time interception of communications	Wiretap Act (18 USC §§2510-22) FISA (50 U.S.C. §§ 1801 et seq.)	Pen Register Statute (18 USC §§3121-27) FISA (50 U.S.C. §§ 1801 et seq.)
Access to stored communications	ECPA (18 USC §§2701-12) FISA	ECPA FISA

cyber defense. As described in Section 3.2, the *Communications Act of 1934* also regulates divulging certain communications and information pertaining to communications.

- The *Electronic Communications and Privacy Act of 1986* (ECPA) amended the Wire Tap Act in a variety of ways. For example, it added statutory protections for stored electronic data in the *Stored Communications Act,* and for data derived from "pen registers" and "trap and trace devices" that pertains to the origin and destination (but not the content) of certain communications in the *Pen Register Statute.* [31] Those provisions set forth the procedures by which governmental authorities may obtain access to such communications and communications-related data, and also include exceptions for certain service providers and other activities that apply in the cybersecurity context.

- The *Foreign Intelligence Surveillance Act* (FISA) imposes criminal penalties upon and authorizes civil suits against any person who intentionally *engages in electronic surveillance under color of law* in the absence of statutory or other authorization and against persons who intentionally use or disclose information so acquired.

- Various states have enacted laws that may limit the interception of electronic communications and the use or disclosure of such intercepted communications. Some may argue that these laws and related judicial doctrines restrict the ability of carriers, ISPs, and others to act as part of a coordinated cyber defense effort.

- The *Privacy Act of 1974* prevents Federal Government departments and agencies from releasing personally identifiable information (PII). Specifically, the Privacy Act states, *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.* Certain sector-specific privacy laws may also restrict public-private information sharing, such as the *Gramm-Leach-Bliley Financial Services Modernization Act,* which focuses on the financial services sector, and the *Health Insurance Portability and Accountability Act,* which focuses on the health sector.

3.2 Regulatory Considerations

Under Section 222 of the *Communications Act of 1934,* as amended, and the FCC's implementing regulations, telecommunications carriers and providers of interconnected Voice over Internet Protocol (VoIP) service have a duty to protect the confidentiality of customer proprietary network information. [32] Telephone companies and providers of interconnected VoIP service may use, disclose, or permit access to customer information in these circumstances:

- As required by law;

- With user approval; and

- In providing the service from which the customer information is derived.

The FCC requires telecommunications service providers and interconnected VoIP providers to file certification stating whether or not they are in compliance with the FCC's Customer Proprietary Network Information rules. The certification must include a statement demonstrating compliance in specific categories.

Contractual Considerations

Telecommunications service providers, ISPs, and other IT companies may face contractual barriers that prevent them from sharing cybersecurity data with the Government. For example, contractual provisions might be interpreted in some circumstances as barring service providers from sharing detailed cybersecurity data that reveals the identity of the providers' customers. If a service provider inadvertently divulges proprietary or other information that may damage a customer's reputation, the service provider might be sued for breach of contract for damages allegedly suffered by the client or others. Major Government customers, however, may wish to modify their contracts with owners and operators and develop contractual provisions that would allow owners and operators to share cybersecurity data within the proposed JCC capability.

3.3 Current Case Law

Theory of Negligent Enablement

Various Federal and state laws and regulations, tort law, international law, evidentiary requirements, and contractual commitments contribute to the legal standards for maintaining information security. Through case law, courts are establishing a 'negligent enablement' legal precedent, which finds liability for companies that neglect to protect data in their custody. For example, if a company neglects to patch a known vulnerability in its network within a timely manner, and customer data is vulnerable, lost, or stolen, the company may be liable. [33] As a result of this legal precedent, owners and operators are increasingly hesitant to share cybersecurity data that may reveal known vulnerabilities in their networks; nor are they eager to share information regarding the company's actions or inactions in addressing the vulnerability. As envisioned during Phase I, sharing aggregated and anonymized cybersecurity data will not expose companies to liability concerns of this type because specific network vulnerabilities will not be revealed. However, as more detailed information is shared in the JCC's subsequent development phases, such as threat and vulnerability data, owners and operators may have liability concerns arising from the 'negligent enablement' precedent.

3.4 Models for Liability Protection

Before implementing Phase II, the Government should consider adopting legislation that would clearly provide liability protection for acquiring, using, and sharing more detailed cyber data, or that would, at a minimum, clearly state that the existing statutory exceptions apply to such activity. As to the former, there are at least three statutes that serve as models for such liability protection:

- The *Support Anti-terrorism by Fostering Effective Technologies Act of 2002* (SAFETY Act); [34] and
- The *Year 2000 (Y2K) Readiness and Responsibility Act of 1999.* [35]

The SAFETY Act provisions provide Federal procurement credits and a safe harbor from civil liability for those companies who can demonstrate compliance with market generated best practices for cyber security. Industry organizations such as the Internet Security Alliance have recommended that Congress adopt a "Cyber Safety Act" based on the Safety Act model. They believe this new act would provide a coherent and comprehensive approach to liability, creating explicit Federal support for incentives that encourage private sector investment in improved security and protection of the Internet.

Another model for cyber security liability protection concerns is the *Y2K Readiness and Responsibility Act of 1999.* This law established protections for companies from potential unfounded or frivolous lawsuits stemming from 'millennium glitches.' Specifically, the law requires a 90-day notification period, places caps on punitive damages, establishes proportional liability, and encourages alternative dispute resolution. The JCC capability may require liability protection similar to those found in both laws.

3.5 International Issues

As a result of the borderless nature of cyberspace and the instantaneous communications it creates, the JCC must engage with members of the international community, including multinational organizations and foreign-owned network service providers. Moreover, private sector entities that operate in foreign countries must ensure that all of their cybersecurity activities conform to applicable foreign legal requirements.

Prior NSTAC Recommendations

In its 2007 *NSTAC Report to the President on International Communications,* the NSTAC reviewed the legal and policy framework underpinning international communications. [36] The existing legal framework consists of treaties, conventions, bilateral dialogues, Mutual Recognition Agreements, Federal Trade Agreements, memoranda of operations, national plans, and other legal instruments. The NSTAC concluded that adequate cyber defense could only occur through international cooperation. The NSTAC considers the recommendations in that report to be crucial in developing the JCC capability.

With respect to natural disasters and physical events having cyber consequences or effects, the NSTAC noted in its 2006 *Global Infrastructure Resiliency Report* [37] that the undersea cable infrastructure carries approximately 95% of the international traffic, including Internet traffic, and that restoration of that infrastructure requires international cooperation. The NSTAC believes that the Federal Government should review these recommendations and consider its appropriate role in the protection and security of that infrastructure.

Implications in Europe

Analysis and response to cross-border cyber incidents requires sharing information among countries. However, some countries have legal restrictions on the acquisition, use, and sharing of this data, particularly if the country considers the data to be PII.

Article 25 of the European Union (EU) *Data Protection Directive* permits the transfer of PII to a non-EU country only if the European Commission has determined that the non-EU country ensures an adequate level of protection. As a whole, U.S. privacy and information protection law does not meet the Commission's standards. However, EU PII can still be shared with the United States under certain contractual arrangements by which the receiving U.S. entities agree to data processing and sharing constraints that meet the *Data Protection Directive's* requirements. For example, air carriers operating flights to or from the United States or across U.S. territory have contractual agreements that permit the carriers to share EU passenger name records (PNR) data with U.S. customs authorities. In addition, U.S. entities that voluntarily certify to the U.S.-EU Safe Harbor Framework may receive EU PII. Many non-EU countries—such as Australia, Argentina, Canada, and Switzerland—have adopted privacy laws similar to the EU's law.

The NSTAC believes that any future legal review and assessment of foreign laws governing the acquisition, use, and exchange of data and PII would facilitate the success of the JCC. The review may determine that the JCC requires a safe harbor provision similar to the PNR Agreements.

3.6 Legal Conclusions

To facilitate information sharing without violating these legal requirements, many service providers have developed policies and procedures to sanitize and aggregate cybersecurity data so that it can be shared with the Government without disclosing PII. The NSTAC believes that these procedures to remove the source and content of IP traffic are an intermediary step that can improve collaboration between the Federal Government and the private sector. Although the JCC's desired end state includes the ability to share the full contents of malicious Internet traffic, the NSTAC recognizes the need for explicit legal authority to share more detailed cybersecurity data with the Federal Government because this increased information sharing may expose PII. For the JCC's Phase I build-up, sanitized and/or aggregated data is sufficient to accommodate the center's initial needs. No new legal authorities are required for Phase I implementation. However, follow-on phases may require additional legal guidance or authorities.

No new legal authorities are required for Phase I implementation. However, follow-on phases may require additional legal guidance or authorities.

4 Findings and Conclusions

The NSTAC recommendations presented in Section 5.0 are based on the CCTF's findings with respect to the need for a coordinated cyber incident detection, prevention, mitigation, and response capability and the CCTF's approach for addressing that need. The NSTAC finds that:

- Today, an adequate national operational capability to respond to the current growing cyber threat does not exist.

- Various entities have carried out cyber attacks against cyber systems and underlying infrastructures. Future concerted cyber attacks against U.S. national infrastructures could be severe or catastrophic. The threat of natural disasters and disruptive physical events, such as cable cuts or

train derailments can significantly impact the cyber environment with long term effects.

- Government and private sector subject matter experts recognize the urgent need for and value of a 24/7 public-private sector collaborative cyber incident detection, prevention, mitigation, and response capability. A phased implementation approach will allow enhanced capabilities to be implemented in an affordable and efficient manner.

- There is an urgent need to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors. The need for this capability is growing over time.

- Previous reports recommended establishing a joint coordination center where the public and private sectors could share cybersecurity information.

- The principal required feature of the Joint Coordinating Center must be rich, timely, bi-directional sharing of actionable information between the public and private sectors to detect, protect, mitigate, and respond to cyber threats.

- There is a lack of clear authority and budget responsibility for a public-private cyber collaboration capability; cyber collaboration capabilities currently exist, but are largely uncoordinated. This is the central issue that must be addressed.

- Successful models of public-private sector collaboration currently exist in practice, such as the long history of the NCC for communications-related matters. The NCC model operates within the existing legal and policy frameworks, and should be leveraged as an integral element for future public-private cyber security collaboration.

- Planning and execution of national cyber incident detection, prevention, mitigation, and response capability requires joint participation of many domestic public and private sector organizations, as well as international entities. Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities. Combining all stakeholders into a single Government funded/equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution.

- The JCC requires a robust, resilient and secure communications system with the critical infrastructure and key resources owners and operators to facilitate the cyber incident detection, prevention, mitigation and response capability.

- Tools, techniques, methods, and procedures must keep pace with and anticipate a rapidly evolving threat.

- No new legal authorities are required for Phase I implementation. Follow-on phases may require additional legal guidance or authorities.

5 Recommendation

Based on the authorities and responsibilities established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* the NSTAC recommends to the President to direct the establishment of a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability to address cyber incidents of national consequence.

To establish this capability, the NSTAC recommends the following:

- Create a Joint Coordinating Center (JCC) as the authoritative place for operational coordination with the private sector critical infrastructure and key resources owners and operators.

  - Assign Government and private sector representatives to develop the initial JCC CONOPS.

  - Provide full JCC functionality on a phased implementation timeline.

- Build on the National Coordinating Center model integrated with the U.S. Computer Emergency Readiness Team model and create a joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability to address a full range of cybersecurity needs.

- Provide a dedicated interagency management structure to govern Federal involvement, including designation of a single, authoritative, and accountable office within the Executive Office of the President. This office should have budgetary and management authority across the Federal cybersecurity enterprise.

- House the JCC in a Government-funded and equipped facility.

- Establish mechanisms for the U.S. Government and the private sector to protect proprietary information and intellectual property, and to mitigate anti-trust concerns.

- Provide resilient, redundant, and secure communications to coordinate across all engaged entities and sectors.

- Before Phase II implementation, conduct antitrust review.

▶ Recognize the private sector as a trusted partner.

- Conduct a joint public-private sector review to identify any existing mechanisms for robust information sharing.

- Fully integrate private sector participants into the JCC operational capability on the same basis as government participants.

- Develop a mechanism and procedures to conduct full, bi-directional information sharing among all JCC participants.

- Provide tools and system access to all JCC participants to establish a fully collaborative working environment.

Footnotes

1 See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force.* October 1990; *NSTAC Network Security Task Force Report.* July 1996; *The NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises.* November 2001; *Next Generation Networks Task Force Near Term Recommendations Working Group Report.* March 2005; *NSTAC Next Generation Networks Task Force Report.* March 2006; and the *NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President.* November 2008.

2 This report will refer to the joint, integrated public-private, 24/7 operational cyber incident detection, prevention, mitigation, and response capability simply as the "cyber incident DPMR capability." Each term (detection, prevention, mitigation, and response) is defined in Appendix A, Glossary of Terms.

3 *Critical Infrastructure: the assets, systems, and networks, whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key Resources: publicly or privately controlled resources essential to the minimal operations of the economy and government. (http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm).*

4 *The NSTAC does not formally comment on pending legislation, but the NSTAC acknowledges that the U.S. Congress is considering many of the issues discussed in this report through proposed legislation. Given the changing nature of bills during the legislative process, the NSTAC notes these developments and will track their progress.*

5 "Blaster worm linked to severity of blackout," *ComputerWorld,* August 29, 2003.

6 "Vast Spy Systems Loots Computers in 103 Countries," *New York Times,* March 28, 2009.

7 http://www.confickerworkinggroup.org/wiki/.

8 *NSTAC Report to the President on Global Infrastructure Resiliency,* October 2006.

9 Electromagnetic pulse (EMP) attacks present a less significant direct threat to telecommunications than it does to the National Power grid, but would nevertheless disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's telecommunications systems in the region exposed to EMP (which could include most of the United States). EMP attacks could damage a functionally significant portion of the Electric Power Grid, resulting in prolonged power- and synergistic system-outages. Dr. William R. Graham, Chair, Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. July 10, 2008. (http://armedservices.house.gov/calendar_past_hearings.shtml).

10 *The President's National Strategy to Secure Cyberspace,* Executive Office of the President (2003).

11 *Tiger Team Report,* Department of Homeland Security (2007).

12 *NSTAC Next Generation Networks Task Force Report* (March 28, 2006).

13 Like the physical infrastructure of roads, bridges, power grids, telephone lines, and water systems that support modern society, 'cyber infrastructure' refers to the distributed computer, information, and communication technologies combined with the personnel and integrating components that provide a long-term platform to empower the modern scientific research endeavor. (http://www.nsf.gov/od/oci/reports/toc.jsp).

14 See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force.* October 1990; *NSTAC Network Security Task Force Report.* July 1996; *The NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises.* November 2001; *Next Generation Networks Task Force Near Term Recommendations Working Group Report.* March 2005; *NSTAC Next Generation Networks Task Force Report.* March 2006; and the *NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President.* November 2008.

15 See: *Network Security Scoping Task Force Report: Report of the Network Security Task Force.* October 1990; *NSTAC Network Security Task Force Report.* July 1996; T*he NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises.* November 2001; *Next Generation Networks Task Force Near Term Recommendations Working Group Report.* March 2005; *NSTAC Next Generation Networks Task Force Report.* March 2006; and the *NSTAC Next Generation Networks Implementation Annex Working Group Letter to the President.* November 2008.

16 *NSTAC Response to the Sixty-Day Cyber Study Group.* Section 3.1. March 12, 2009.

17 Ibid. Section 4.5.

18 See Appendix C for a list of Government officials and private sector representatives who met with the CCTF.

19 As a result of the 2007 DHS *Tiger Team Report,* DHS has efforts underway to develop a collocated, coordinated operational capability. The NSTAC envisions that its proposed cyber incident DPMR capability may build on these efforts.

20 The term "key sectors" refers to the banking and finance, communications, energy, and IT sectors.

21 "If the partnership between the Federal Government and private sector is to be successful, another key requirement is establishing a permanent physical location or forum so that critical and non-critical sectors can interface with one another and their Federal counterparts. This is essential to developing and maintaining long-term collaborative relationships." *A Review of the Top Officials 3 Exercise,* DHS OIG Report OIG-06-07, p. 24 (Nov. 2005).

22 The term 'controlled communication mechanisms' refers to real-time, managed bridges and Web tools for information sharing.

23 In response to the President's 60-day Cyber Review, the NSTAC provided input and recommendations; the recommendations in this report are consistent with those recently provided in the NSTAC's support of the 60-day Cyber Review.

24 This issue is currently being addressed through the Project 12 activities under the Comprehensive National Cyber Initiative.

25 NSTAC LRTF Report. *Barriers to Information Sharing,* September 2003.

26 *Sherman Antitrust Act of 1890, July 2, 1890,* ch. 647, 26 Stat. 209, 15 U.S.C. § 1–7.

27 *The proposed JCC could be modeled on the NCC. The NCC participants share real-time information about communications networks. For the NCC, the Department of Justice issued a letter ruling stating that NCC's collaborative activities do not violate antitrust laws. Specifically, the letter ruling determined that the NCC collaborative activity was one which "would enable the industry to provide collectively that which each member of the industry could not provide individually, i.e., a nationwide, interoperable system of independent carrier networks in which the resources of all are available to meet this Nation's NS/EP needs." See Letter from the Office of Attorney General,* June 1, 1983, to Lt. Gen. William J. Hilsman, Manager, NCS.

28 In the future, effective coordination of information sharing would be solidified if specific legal protections were enacted for cyber defense activities designed to acquire, use, and appropriately share relevant information, including through measures designed to monitor, intercept, use and disclose aspects of Internet and other IP communications.

29 Table 2 is based on information taken from Joel M. Schwarz, DOJ, and was modified by the NSTAC Task Force. Joel M. Schwarz, DOJ, Computer Crime and Intellectual Property Section, Criminal Division. *Cyber Security—the laws that Govern Incident Response.*

30 Section 2701 (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; and USC 2511 (2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

31 *§2701 – The Stored Communications Act of 1986* focuses on unlawful access to 'stored wire and electronic communications and transactional records.' According to the statute, anyone who *intentionally accesses without authorization a facility through which an electronic communication service is provided or… intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system is subject to prosecution. §3121 – The Pen Register Act of 1986* governs real-time monitoring, but not collection, of communications traffic data. Carriers and ISPs are required to provide content if served with a court order. This statue was designed to apply to traditional telecommunications networks and to enable law enforcement officers to capture the originating and terminating telephone numbers of phone calls made to and received by an individual, but not the content of those calls. The FCC expanded the scope of the *Communications Assistance for Law Enforcement Act* to include the interception of information provided over the Internet. The Pen Register Act has since been applied to Internet technologies, allowing law enforcement officers to monitor the source and destination of Internet Protocol traffic. CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities. *Telecommunications carriers are identified as common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service. (http://www.fcc.gov/calea/).*

32 *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers; Use of Customer Proprietary Network Information and Other Customer Information;* IP-Enabled Services, 22 FCC Rcd 6927 at ¶ 54.

33 *In 2003, the State of California was the first state to pass a law mandating that companies or other organizations maintaining personally identifiable information (PII) must notify affected citizens if their data has been lost, stolen, or shared without proper permission. Regulators and enforcement agencies must also be notified following a data breach. Following California's example, 34 other states have passed similar data breach notification laws that impose a 'duty to warn' on companies and organizations that maintain PII.*

34 *Support Anti-Terrorism by Fostering Effective Technologies Act of 2002,* 6 U.S.C. §§ 441-44 (2006).

35 *Year 2000 (Y2K) Readiness and Responsibility Act of 1999,* Public Law 106-37.

36 *NSTAC Report to the President on International Communications,* August 16, 2007.

37 *NSTAC Report to the President on Global Infrastructure Resiliency,* October 2006.

Glossary of Key Terms

Glossary of Key Terms

Critical Infrastructure
The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on national, homeland, or economic security, public health or safety, or any combination thereof

Cyber Infrastructure
The distributed computer, information and communication technologies combined with the personnel and integrating components that provide a long-term platform to empower the modern scientific research endeavor

Detection
Developing an understanding of normal network traffic volume and flow using independent sources will help the JCC participants detect anomalies. Stakeholders will work with partners to obtain external data on threats and vulnerabilities.

Key Resources
Publicly or privately-controlled resources essential to the minimal operations of the economy and government

Mitigation
Developing the mitigation tools and technology will help stakeholders to address cyber incidents, while ensuring stability within other unaffected networks.

National Security and Emergency Preparedness (NS/EP) Communications
Communications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States. [38]

Next Generation Networks
The NGN will logically consist of applications that deliver services, the services provided to users, and the underlying transport networks…The NGN itself is a capability that will enable many services and applications. Some services will be provided by the network; other services may be external to it, but will depend on it. NGN user-centric services will be delivered over various networks, some of which (such as private customer premises networks and mesh networks) lie outside the wide scope of the Public Network. However, there is no single or universally accepted definition of the NGN in existence. The term NGN is not intended to represent any single configuration or architecture. Instead, it represents the set of converged networks…expected to arise that will transparently carry many types of data and communications and allow delivery of services and applications that are not coupled to the underlying network. However, it is possible to note several key NGN elements or attributes over which there is little, if any, dispute. [39]

Personally Identifiable Information (PII)
Information that can be used to distinguish or trace an individual's identity (such as their name, social security number, or biometric records), either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Prevention
Developing proper interdiction guidance for prevention activities. Prevention activities include bi-directional information sharing within the IT and communications sectors, and with government (Federal, state and local) and international agencies.

Response
Organizing teams, processes, and procedures will help stakeholders to coordinate internal and external sources to respond to and recover from incidents.

Footnotes

38 NCS Directive 3-1, *Telecommunications Operations Telecommunications Service Priority (TSP) System for National Security and Emergency Preparedness.*

39 *NSTAC Report to the President on Next Generation Networks,* March 28, 2006.

Suggested Phased Approach Implementation

Suggested Phased Approach Implementation

The table below depicts a possible implementation process for the phased approach:

Suggested Phased Approach Implementation		
Phase	Timeframe	Activity
Phase 0	Within 60 Days	Complete initial CONOPS.
Phase I	Within 90 days of CONOPS approval	Implement Phase I joint CONOPS to provide cyber situational awareness and a common operational picture.
		Integrate core Phase I JCC members. [40]
		Deploy controlled communication mechanisms for information sharing and collaboration.
		Identify, develop, and integrate capabilities to establish an operating environment. Some capabilities include rapid collaboration, mitigation, trend analysis, monitoring via watch functions, and shared products.
		Accept/procure data inputs/feeds from other organizations – SANS Internet Storm Center (ISC), Symantec Corporation, McAfee, and others as necessary.
		Ensure legal considerations in Section 3.0 are aligned with future planned activities.
		Establish/review Phase I metrics to measure progress and inform the development of further phases.
Phase II	Within one year of CONOPS approval	Establish training and exercise functions.
		Integrate with other organizations – National Security Agency Threat Operations Center (NTOC), Intelligence Community Incident Response Center (IC-IRC), State/local, tribal, international partners.
		Invite representatives from remaining 18 CIKR sectors.
		Define requirements for additional operational capabilities, including more robust information sharing between the public and private sectors; gather additional legal guidance as needed.
		Update and enhance CONOPS based on experience.
		Ensure legal considerations in Section 3.0 are aligned with future planned activities.
		Establish/review Phase II metrics to measure progress and inform the development of further phases.
Phase III	After one year of CONOPS approval	Define requirements for additional operational capabilities, including more robust information sharing between the public and private sectors; gather additional legal guidance as needed.
		Update and enhance CONOPS based on experience.
		Ensure planned activities are consistent with legal considerations in Section 3.0.
		Establish metrics to measure progress and inform the development of further phases.

Important factors for success include:

- Adequate and appropriate resources (for example, funding, personnel, and collaboration tools);
- Core physical facility with appropriate security and resilient communications and utilities;
- Voluntary private sector representation initially from the banking and finance, communications, energy, and IT sectors with full physical access to the facility; virtual access initially for other sectors;
- Extended virtual participation from both the Government and the private sector over time; and
- Controlled communications mechanisms for information sharing among the private sector and government partners.

Footnotes

40 Core Phase I JCC members include those entities listed in Section 2.3.

Studies and Reports

Studies and Reports

NSTAC Reports

2008 Next Generation Networks Implementation Annex Working Group Letter to the President

In this letter, the NSTAC stated it had re-examined the previous 2006 Next Generation Networks (NGN) Report to: identify and review current Federal Government efforts that address issues in the report's recommendations; and identify gaps among the 2006 *Report* recommendations, current NGN needs related to the provisioning of NS/EP communications, and existing Federal Government activities, and to provide follow-up recommendations to ongoing work and to enhance future Federal NGN NS/EP activities and implementation actions.

2007 NSTAC Report to the President on International Communications

A key recommendation of the *NSTAC Report to the President on International Communications* was for *DHS to coordinate international planning and development with the appropriate Federal Agencies for adoption of a global framework incorporating operational protocols and response strategies.* This report specified that this framework should examine, *with the help of private sector partners, existing U.S. laws and policies that could prevent service providers and other stakeholders from taking the necessary proactive measures to restore service and prevent harm to NS/EP users for government essential operations during a crisis.*

2006 NSTAC Report to the President on the National Coordinating Center (NCC)

Key recommendations from the NCC report include requesting expanding *the NCC to include both communications and IT companies and organizations. This would be a cross-sector public-private sector facility with a round-the-clock watch, and would be brought up to full strength during emergencies.* Additionally, the report recommended engaging *the private sector in critical infrastructure protection activities by increasing the flow of threat information to the private sector, facilitating private sector participation in impact analyses, and clarifying policies for the protection of private sector information.* Finally, the report concluded by improving *the Federal Government's cyber response strategy to delineate roles and responsibilities of Government and the private sector in the National Response Plan, aligning communications and cyber operations centers, and enhancing relationships with international computer emergency readiness teams.*

2006 Next Generation Networks (NGN) Task Force Report

A key recommendation of the NGN Report was the creation of *an inclusive and effective NGN incident response capability that includes a Joint Coordinating Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors.*

2005 Next Generation Networks Task Force Near Term Recommendations Working Group Report

This report focuses on convergence and how the Federal Government will meet its needs for national security and emergency preparedness (NS/EP) communications. The report discusses how the Government can meet NS/EP requirements and address emerging threats using the NGN. Many of the recommendations focused on cross-government coordination to track NGN activity, collaborating with the private sector, and providing greater support to private sector efforts to determine NS/EP risks during convergence.

2003 Legislative and Regulatory Task Force Report on Barriers to Information Sharing

The Legislative and Regulatory Task Force *Report on Barriers to Information Sharing* produced a series of recommendations for the Federal Government action designed to improve information sharing between the public and private sectors.

2001 The NSTAC's Input to the National Plan, *An Assessment of Industry's Role in National Level Information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crisis.*

This report focuses on the need for a recognized, authoritative, national-level capability to disseminate warnings and facilitate response and mitigation efforts for cyber crises across the Nation's infrastructures. Key elements of such a capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination.

1990 Network Security Scoping Task Force Report: Report of the Network Security Task Force

Recommendations from this report include identifying a mechanism for security information exchange and providing steps for Government agencies to improve intelligence information sharing to the private sector and led to the creation of the National Security Information Exchange.

Department of Homeland Security (DHS) Reports and Plans

2009 National Infrastructure Protection Plan (NIPP)

The NIPP addresses the requirements set forth in Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection,* and provides the overarching approach for integrating the Nation's many CIKR protection initiatives into a single national effort. It sets forth a comprehensive risk management framework and clearly-defined roles and responsibilities for DHS; Federal Sector-Specific Agencies; and other Federal, State, regional, local, tribal, territorial, and private sector partners implementing the NIPP.

2008 *Comprehensive National Cybersecurity Initiative's* Project 12 Report

A key recommendation from the Project 12 Report, *Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships,* recommended expanding the joint operational capability of US-CERT and NCC to include private sector CIKR sector participation. This effort would eventually include voluntary participation from all 18 CIKR sectors, as determined appropriate by each of the sectors. Co-location of private sector partners could be physical or virtual. DHS is currently implementing the co-location of the NCC and US-CERT.

2007 Department of Homeland Security *Tiger Team Report*

This report was developed in 2007 by Government representatives from NCS and NCSD and industry representatives from the NCC/Communications and IT Information Sharing and Analysis Centers following the NSTAC 2006 Next Generations Report. The 2007 report provided guidance and recommendations on why and how DHS could lead the government and industry in building a fully integrated operational capability to perform cyber and communications security missions in an environment characterized by the convergence of the IT and Communications sectors. The report outlined a three-phased implementation: Phase I called for collocating US-CERT and NCC Watch in a common facility; Phase II called for integrating the operational capabilities of the US-CERT and NCC Watch to create a single 24/7 operational entity that incorporates the current missions of US CERT and NCC Watch, and met CS&C's National-level mission requirements; and Phase III called for inviting other sectors to send representatives to the joint operations center. Phase I was implemented in late 2007/early 2008. The recommendations associated with the Tiger Team's Phase II are consistent with this report's Phase I capabilities.

2007 Information Technology (IT) Sector Specific Plan (SSP)

The IT Sector Specific Plan notes that *public and private sector security partners have an enduring interest in assuring the availability of the infrastructure and promoting its resilience. The IT SSP represents an unprecedented partnership and collaboration between the IT public and private sectors to address the complex challenges of CIKR protection. Public and private sector organizations each represent and bring unique capabilities to the partnership, and derive value from the exchange. Successful CIKR protection is the commitment of IT Sector public and private sector security partners to share information and provide the tools and capabilities necessary for an effective partnership.*

Other Reports

2009 Congressional Research Service Report: *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*

This report discusses the legal issues and addresses policy considerations related to the Comprehensive National Cybersecurity Initiative, specifically focusing on legal authorities for Executive Branch response to cyber threats, Congressional constraints on Executive action, and policy considerations.

2008 Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency

A key recommendation from the *CSIS Commission on Cybersecurity for the 44th Presidency* focused on redesigning and recasting the Government's relationship with the private sector to promote better cybersecurity.

2008 Internet Security Alliance *Cyber Security Social Contract*

A key recommendation of the Internet Security Alliance's report was the creation of *a social contract wherein government provides incentives for the private sector to make cyber security investments that are not justified by current business plans is a pragmatic alternative.* The report *identified what the government can best do, both long and short term to address these needs and specifies a series of steps the new Administration and Congress can take toward establishing a coherent, pragmatic, effective and sustainable system of cyber security.*

2003 President's National Strategy to Secure Cyberspace

The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. The *National Strategy to Secure Cyberspace* outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the Federal Government departments and agencies that have roles in cyberspace security. It also identifies steps that State and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The *Strategy* highlights the role of public-private sector engagement. The document provides a framework of contributions to secure our parts of cyberspace.

Presentations to the Cybersecurity Collaboration Task Force

Presentations to the Cybersecurity Collaboration Task Force

Government Presenters	
Presenter	Role
Dr. Peter Fonash	Acting Deputy Assistant Secretary Cybersecurity and Communications, Chief Technology Officer, and Acting Director National Cybersecurity Division (NCSD) Office of the Assistant Secretary for Cybersecurity and Communications Department of Homeland Security (DHS)
Mr. Jeffery Goldthorp	Chief of the Federal Communications Commission's Communications Systems Analysis Division in the Public Safety and Homeland Security Bureau
Ms. Mischel Kwon	Director, United States Computer Emergency Readiness Team (US-CERT)
Mr. Brett Lambo	Director, Cyber Exercise Program, NCSD
Ms. Jenny Menna	Acting Director, Critical Infrastructure Cyber Protection and Awareness, and Acting Director, Global Cyber Security, NCSD, DHS
Ms. Victoria Morgan	Director, Intelligence, Interagency and Networks, Defense Industrial Base (DIB) Cyber Security Task Force
Ms. Jordana Siegel	Director, Outreach and Awareness, NCSD, DHS

Industry Presenters	
Presenter	Role
Ms. Tiffany Jones	Director, Public Policy and North American Government Relations, Symantec
Mr. David Kessler	Senior Corporate Counsel, Symantec
Mr. Marcus Sachs	Executive Director, Government Affairs National Security Policy, Verizon
Mr. Jonathan Spear	Vice President and Deputy General Counsel, Verizon

Other Presenters	
Presenter	Role
Mr. Marcus Sachs	Director, SANS Internet Storm Center
Mr. Matt Ziemniak	Program Director, Cyber Operations Division, National Cyber-Forensics Training Alliance (NCFTA)

Participant List

Task Force Members

AT&T, Incorporated
Ms. Juliana Thomas

Bank of America Corporation
Mr. Larry Schaeffer

Boeing Company
Mr. Bob Steele

Computer Sciences Corporation
Mr. Guy Copeland

Harris Corporation
Mr. Richard White

Juniper Networks, Incorporated
Mr. Robert B. Dix, Jr.

Lockheed Martin Corporation
Gen. Charles Croom (Ret.)

Microsoft Corporation
Ms. Cheri McGuire

Nortel Networks Corporation
Dr. Jack Edwards

Qwest Communications International, Incorporated
Ms. Kathryn Condello

Raytheon Company
Gen. Bill Russ (Ret.)

Rockwell Collins, Incorporated
Mr. Ken Kato

Telcordia Technologies, Incorporated
Ms. Louise Tucker

VeriSign, Incorporated
Mr. William Gravell

Verizon Communications, Incorporated
Mr. Michael Hickey

Other Participants

AT&T, Incorporated
Ms. Rosemary Leffler
Mr. John Markley

Boeing Company
William Reiner

Computer Sciences Corporation
Mr. Kenneth Thomas

Deloitte
Col. Gary McAlum (Ret.)

George Mason University Law School CIP
Ms. Maeve Dion

Harris Corporation
Ms. Tania Hanna

The Mitre Corporation
Mr. Scott Tousley

Netmagic Associates LLC
Mr. Tony Rutkowski

Lockheed Martin Corporation
Dr. Eric Cole
Mr. Arnie "AJ" Jackson
Mr. James "Tom" Prunier

Qwest Communications International, Incorporated
Mr. Curtis Levinson

Raytheon Company
Mr. Charles McCaffrey

Science Applications International Corporation
Mr. Hank Kluepfel
Mr. Steve Lines

Sprint Nextel Corporation
Ms. Allison Growney

Unisys
Ms. Patricia Titus

Valley View Corporation
Mr. Dan Bart

Verizon Communications, Incorporated
Mr. Jim Bean
Mr. Marcus Sachs

U.S. Government Personnel

Department of Homeland Security
Ms. Kathleen Blasco
Mr. Kevin Dillon
Mr. Ryan Higgins
CAPT Alice Rand
Mr. Matt Shabat
Ms. Jordana Siegel
Mr. Will Williams
Ms. Chris Watson

Department of Defense
Lt. Col. Susan Camoroda

Federal Communications Commission
Mr. Gregory Cooke
Mr. Richard Hovey

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Identity Management Strategy

May 21, 2009

Table of Contents

Executive Summary

At the direction of the Executive Office of the President and following a comprehensive scoping effort, the President's National Security Telecommunications Advisory Committee (NSTAC) established the Identity Issues Task Force in November 2008 to explore the role of the Federal Government in Identity Management (IdM) and how it could serve as a catalyst for broad implementation. As such, the NSTAC proposes a broad approach to assist the United States in achieving a national, comprehensive IdM strategy through a broad and enduring partnership between Government and industry. Internally, the Federal Government can implement IdM policies and technologies to improve privacy, security, and confidence in its own networks and services. Beyond that, a need has emerged for a national, comprehensive IdM strategy that would recognize and protect the roles and interests of private citizens and commercial participants while enabling collaboration among key stakeholders.

A comprehensive national vision and strategy will help create an IdM infrastructure capable of managing digital identities in the evolving electronic environment facilitating confidence and trust. This new IdM environment could have profound political and social implications, significantly improving how citizens interact while simultaneously meeting their basic expectations of privacy and anonymity. In addition, a comprehensive national vision and strategy for IdM will substantially enhance the overall security and integrity of the national communications infrastructure.

During emergencies, Federal, State, and local governments rely on the availability of trusted Internet and other communications systems. National security/emergency preparedness (NS/EP) users have the same characteristics as most Internet Protocol (IP) network users—they are nomadic and demand access to all services at any time. However, they also differ from ordinary users in that they demand priority access to these services so they can respond to events where lives and property are in imminent danger. Consequently, network operators and service providers must be able to verify the identity of NS/EP emergency responders. These providers need a mechanism to establish trust in an NS/EP environment, and IdM provides that mechanism. A lack of IdM capabilities could result in a situation where unauthorized users have access to NS/EP priority services, perhaps interfering with an emergency responder's ability to use those services to fulfill the mission. Consequently, it is in the Government's best interest to pursue the development of a federation of interoperable IdM processes. Such a federation of interoperable IdM processes would enhance identity trust, awareness and education among end users, providers and devices. This federation would strengthen trust relationships and enhance the Nation's security. Such a federation would involve three operational characteristics: (1) interoperability; (2) Trust Anchors; and (3) Choice-based participation. A strong IdM system, based on robust trust in the Internet infrastructure and design, increases consumer confidence and ensures the Government's ability to rely on the Internet and other communications systems for commercial activities and security operations.

> The evolving threat environment, coupled with the increasing reliance on communications networks, requires the development of a national, comprehensive Identity Management vision, strategy, policy and implementation procedures.

Both Government and the private sector are engaged in this area and are working toward individual solutions to IdM challenges to achieve the goals and overarching objectives for an IdM strategy addressed here. Although these efforts may be individually beneficial, they do not achieve the level of coordination, efficiency, and scope needed to create a holistic, integrated national IdM strategy for the mutual benefit of Government, industry, and society.

Commercial IdM service providers exist today and will likely increase in number, expand their roles and offerings, and develop business opportunities to meet the growing national IdM need. The national IdM strategy must embrace commercial IdM service providers willing to collaborate with the Government to develop standards-based interoperability between Federal and commercial IdM processes.

Privacy and civil liberties are vitally important components of any successful national IdM strategy that includes a federation of interoperable IdM processes. The NSTAC does not define a specific solution regarding how privacy should be integrated into a national IdM framework, but a fully-formed, Choice-based approach is fundamental to meet the citizens' expectations regarding privacy, civil liberties, and the protection of sensitive information, and will warrant further study. Importantly, the details of implementation of how to identify and authenticate users will not be answered in this report, but aspects are discussed to establish the contextual basis for this work and extend support for the NS/EP process. End users must have the ability to make fully-informed choices about the protection and use of their sensitive information. The relationship of these important civil liberties and the benefits of an interoperable IdM process warrant further study.

The recommendations to the President address possible first steps for an approach to identify issues and solutions related to IdM. This report builds upon IdM recommendations of previous task forces, working groups, researchers, and international bodies as referenced within the text herein. In addition, the IdITF considered the extensive IdM research and development (R&D), policy development, and technical research conducted by numerous national and international standards bodies and organizations.

This study is consistent with, and extends the work of, the President's NSTAC on the 60-day review of the Nation's cybersecurity efforts. Based on these efforts, the NSTAC believes a comprehensive national identity strategy would provide the crucial foundation for achieving success in many wide-ranging cybersecurity initiatives. The NSTAC also believes that the current political and policy landscape is ripe for promoting a comprehensive national strategy to improve trusted identification. Implementing such a strategy will impede malicious actors from posing as legitimate users and exploiting these networks, thereby placing NS/EP capabilities and everyday commerce at risk.

In light of these circumstances, the NSTAC concludes that the Government, working collaboratively with the private sector, the public, and interested nations, should develop a comprehensive national IdM vision and strategy that meets the security, business, and personal needs of American society and addresses the organizational, programmatic, legislative, and cultural components of IdM.

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions:*

1. ***Demonstrate personal national leadership in IdM to positively influence the national culture, attitude, and opinion toward IdM.*** Successful development and implementation of a national IdM vision and strategy requires national commitment across Government, industry, and individuals dependent on cyber applications

2. ***Charter a national IdM office under specifically appointed and dedicated leadership, in the Executive Office of the President.*** This office must have powers to integrate and harmonize national IdM policies and processes, including those related to law enforcement and security, as well as physical and logical access controls. This office should seek active private sector participation in developing such policies and processes in order to succeed and to ensure that successful solutions are shared with the private sector, as appropriate.

3. ***Direct the newly created office to develop a coordinated programmatic agenda to implement a comprehensive IdM vision and strategy to address, at a minimum, four component areas, specifically: Government organization and coordination; public-private IdM programs; policy and legislative coordination; and national privacy and civil liberties culture.*** Because no existing Government office or organization is engaged in all areas and issues across the total scope of IdM, new approaches are required to harness the expertise and interests across all areas.

With respect to Governmental organization and coordination, establish a single, authoritative and comprehensive IdM governance process with a dedicated mission and office under an accountable official reporting directly to the President, embracing all Federal policy, technology, and IdM application activities related to both screening and access controls. The established lead official should have control over defined IdM programs and resources across Government, including budget, as needed to advance Federal IdM under a single coherent strategy.

With respect to public-private programs, direct the appropriate Federal Government departments and agencies to work with the private sector to develop and advance a comprehensive and progressive IdM Research and Development agenda, focusing on Government-civil IdM interoperability. This effort should seek to establish interface standards to enable IdM applications to access and securely operate on global communications networks. In addition, this effort should partner with industry to embed IdM solutions in identity-sensitive applications of all kinds, promoting standards-based public-private programmatic collaboration.

With respect to policy and legislative coordination, determine what changes to policy and regulation should be made, and what legislative initiatives should be advocated to move quickly toward national IdM goals. Further, establish policy and a legal framework to support internal Federal activities and streamline Government-civil collaboration and partnership in support of those goals. In particular, the IdM office should pursue legislative efforts to support National IdM governance, organization and authority needs, as appropriate.

With respect to national privacy and civil liberties culture, develop a comprehensive and sustained communications plan to promote IdM reflecting key national and social values and embracing the strong National conviction to protect privacy and civil rights of both initiating and receiving parties as the national IdM strategy is developed and implemented.

All four of these components must be acted upon to achieve needed IdM alignment within Government, and between Government and industry. Collectively, these efforts will provide the Presidential emphasis, streamlined authorities, and broad engagement needed to achieve the beneficial effects of IdM throughout the Nation.

Scope and Purpose

The increasing dependence on communications networks for conducting Governmental, commercial, and social transactions requires participants to establish their identity through digital means. Trusted, strong identification of users, devices, and communications service providers has not been universally adopted in cyberspace. This lack of trusted identification diminishes NS/EP capabilities, endangering national and homeland security as well as individual security and privacy.

The National Security Telecommunications Advisory Committee (NSTAC) proposes a broad approach to enable our Nation to achieve a holistic, comprehensive Identity Management (IdM) strategy through an enduring partnership between Government and industry. The increasing dependence on communications networks for conducting Governmental, commercial, and social transactions requires participants to establish their identities through digital data and potentially physical means. Identity Management (IdM) provides unique characteristics and attributes to any Entity (e.g., people, object, device, or organization). Trusted, strong identification of users, devices, and communications service providers has not been universally adopted in cyberspace. This lack of trusted identification enables harmful and/or malicious activity [1] and diminishes national security/emergency preparedness (NS/EP) capabilities, [2] endangering national and homeland security as well as individual privacy and security. Private sector owners and operators of the Nation's information technology (IT) and communications infrastructure, along with Government, have a vested interest in identifying and deploying solutions to help the Nation reduce the occurrence and impact of harmful activity on communications systems.

IdM covers a broad scope, including both digital and physical identification of individuals, applications, devices, objects, and information.

The purpose of this report is to identify Federal Identity Management (IdM) [3] policies and Government roles and responsibilities most likely to create a large-scale demand for strengthened IdM capabilities and practices by the private sector and individual users. In collaboration with Government and private sector officials and technologists, the President's National Security Telecommunications Advisory Committee (NSTAC) Identity Issues Task Force (IdITF) explored the following topics:

- Functional identity requirements;
- Current Government IdM initiatives;
- Potential impact of IdM on Government priorities;
- Current domestic and international IdM standards adoption; and
- Creation of a process to develop, evaluate, and coordinate national comprehensive IdM strategies.

In the context of this IdM approach, Government and the private sector must commit to improve, to the extent possible, planning and execution in these areas. Sensitivity to public opinion in matters involving personal privacy and the proper roles—and limits—of Government must be taken into account. The recommendations are intended to present strategies and processes that improve privacy, relative to the status quo, while expanding the potential scope and scale of national IdM efforts, through establishing auditable and transparent privacy safeguards. Specifically, the recommendations herein promote a balanced public-private IdM strategic approach offering opportunity for business participation, standards development, and interoperability within and among Government and the private sector entities.

Background

Federal, State, and local governments, international bodies, private sector organizations, and individual end users depend on robust, reliable and functional communications networks for NS/EP and other business and personal needs. The Government and

private sector rely upon these networks [4] increasingly for daily transactions (e.g., the provision of healthcare, emergency response services, commercial activities, and e-Government services). Numerous sources [5] show that these networks—and the governments, people, devices, and the applications that rely on them—are under daily and sustained attacks. These attacks threaten core U.S. national communications objectives, including national security, law enforcement, public safety, and protection of intellectual property, and impair the availability and integrity of communications networks for NS/EP. In addition, they enable hostile disinformation capabilities, denial of service attacks, and malicious virus and spam attacks, all of which result in the general abuse and exploitation of communications networks by nation states and individual actors alike.

The evolving threat environment, coupled with the increasing reliance on communications networks, requires a national, comprehensive Identity Management vision and strategy.

Both criminal and state-sponsored actors try to capture identity information. They subsequently use to gain unauthorized access to systems and information. The absence of strong identity controls makes it easy for them to get the information they need. The most common example of an inadequate identity control is a weak password (which is often 'password'). Captured identity information may be used to spoof communications networks' Authentication [6] processes to gain unauthorized access to networks and information. This increases the potential for theft, fraud, and the manipulation or disruption of finances, intellectual property, and other sensitive information. If information such as dates of birth and social security numbers are used as the basis of identity, and are compromised, recovery is difficult and sometimes impossible.

Recent studies by Government [7] and think tanks [8] have recognized the relationship between cybersecurity and IdM. Although this relationship has not yet been defined or described in detail, it clearly exists and current policy efforts related to broader issues of cybersecurity should be extended to IdM.

Inadequate identity control can negatively affect our communications infrastructure and all those who rely on it. A successful IdM strategy can help protect that infrastructure. As this strategy is adopted, there will be recognizable benefit in every identity-sensitive application. An effective IdM strategy can be a critical enabler for several Federal homeland security priority agenda items, including: [9]

- Protecting information networks;
- Improving intelligence capacity;
- Protecting civil liberties;
- Protecting Americans from terrorist attacks and natural disasters; and
- Protecting and modernizing critical infrastructure.

For example, IdM plays a key role in the healthcare reform agenda, promoting the adoption of online record-keeping and technology innovation initiatives, including widespread broadband access and an open Internet to improve access to healthcare while reducing healthcare costs. [10]

NS/EP, business, and even personal requirements drive the need for IdM and are linked to the evolution of the Internet as a critical infrastructure that supports vital processes in government, business, and society. Transactions often occur over distances, where the sender and receiver do not share a common security framework or risk tolerance. Ubiquitous global networks have permitted the emergence of new functionality and efficiencies, but their full potential cannot be realized without a way to ensure their information is secure and their transactions are with trusted parties. Consequently, the ability of security organizations to differentiate between authorized users and intruders has become imperative.

Beyond network-based concerns, the ability to identify persons and objects for physical access control is part of the total need of IdM. The NSTAC addressed this issue in 2003. [11] The NSTAC's perspective on IdM should apply to both domains. Therefore, all references

to interoperability of processes, applications, and systems in this report apply to both the physical and logical aspects of IdM.

The benefits of IdM extend beyond protecting the infrastructure and its users from malicious actors. Implementation of practical, large-scale IdM processes can also motivate users to take greater advantage of the functionality available, which in turn can stimulate further innovation. The ability to help all stakeholders appreciate these benefits will be essential to success and in some cases will require external advocacy and outreach programs. The benefits include:

- Expanded access to goods, services and information;
- Reduced process latency and error;
- Increased productivity and efficiency; and
- Cost savings.

The ubiquitous nature of the Internet and its application as a tool to meet Government and private sector mission needs underscores the increasing importance of IdM. The current environment requires collaboration among the Government and relevant stakeholders to ensure the development of a comprehensive, national IdM strategy.

The increasing emphasis on cybersecurity, healthcare technology innovation, and financial services initiatives has made key stakeholders interested in a broad IdM approach that addresses the full spectrum of issues and communities. This 'critical mass' has stimulated a greater awareness of IdM concerns, leading to opportunities for IdM policy development and implementation. With this awareness comes a need for Government to implement an outreach effort to ensure individuals have accurate and reliable information about how IdM can help them take full advantage of available technologies.

Privacy

A national IdM strategy must address personal privacy. Requiring identification for anonymous activity (for example, most Web browsing) could pose privacy risks by exposing Personally Identifiable Information (PII) to unauthorized third parties, who could then aggregate the information and link it to particular individuals. However, the implementation of an effective IdM strategy should enhance consumer privacy by increasing consumer control over personal information, strengthening information security, reducing unwanted intrusions such as spam, and improving transparency regarding how information will be used. Successfully strengthening identification processes while preserving privacy and civil liberties requires a delicate balance. To achieve this end, all participants in the design and implementation of a national IdM strategy should embrace the resolution of privacy concerns as a fundamental charge.

The NSTAC does not define a specific solution regarding how privacy should be integrated into a national IdM framework, but a fully-formed, Choice-based approach is fundamental to meet the citizens' expectations regarding privacy, civil liberties, and the protection of sensitive information. The NSTAC believes that all major participants should collaborate on an IdM strategy that establishes rigorous and auditable policy and technology frameworks while simultaneously ensuring identity privacy. This consideration of privacy applies broadly within Government, between the Government and commercially sensitive activities, and across society.

Identity Management and Its Uses

An identity is a representation of an Entity (such as an end user, a subject [as in law enforcement and security applications], an object, a device, or an organization) by which the entity is known in some context. The contexts considered in this report involve a broad array of infrastructures used for communications, transactions, or control of resources or facilities. Any entity may have one or more identity claims. A single identity may also be associated with multiple Entities. IdM includes discovery of and access to authoritative identity sources, and involves the life-cycle management and use of identity data elements to enable Attribution, [12] Authentication, and other identity-based services. IdM provides the means to authenticate the identity claims of Entities requiring identification on communications networks. [13] These claims include multiple roles (such

as citizen, spouse, parent, customer, and patient) and range from commercial to social activities, and require participants to establish their identities through digital identity data and, in some cases, physical means.

The benefits that adoption of a comprehensive national IdM strategy would bring are far-reaching, as highlighted below. [14]

Increasing global complexity has yielded an evolving identity environment reaching across diverse domains. If IdM stakeholders do not address the fundamentals now, then more isolated IdM systems will emerge and it will become far more difficult to adopt viable, comprehensive, interoperable IdM solutions in the future.

Identity Management Benefits

IdM processes and devices must be seen as valuable and useful by end-users. Those processes and devices must provide key positive incentives, such as passing through airports more quickly or gaining direct and secure access to Government systems online, so that voluntarily providing PII offers something of value. Advantages and cost savings will increase as IdM technology becomes more ubiquitous. The development of a comprehensive national IdM strategy would provide significant, tangible benefits to Government, industry, and the general public, such as:

- Reduced identity theft even with increased use of electronic commerce and e-Government;
- Reduced financial loss and improved recovery from identity fraud;
- Increased consumer confidence in Internet Protocol (IP)-based networks should result in the increased use of these networks for commercial transactions and thereby produce greater efficiencies at lower costs;
- Enhanced physical access controls and security screening processes;
- Cost savings through greater adoption of on-line applications for government and commercial services requiring in-person identity verification;
- Recognizable, credible, and interoperable identities being made optionally available for all citizens, following essential industry and Government standards and applicable laws;
- Greater identity attribution without violation of citizens' privacy rights;
- More electronic value chains that can simultaneously promote U.S. innovation and international trade;
- Improved extensibility and interoperability of a smaller family of ID tokens and systems, benefiting both ID-dependent businesses and consumers;
- Streamlined and more secure access to the whole range of identity-sensitive applications, from law enforcement and security screening to e-commerce and access controls, including via Web-based processes never before possible. For example:
  - Secure Internet access to health services with improved privacy of personal medical records
  - Enhanced secure e-pharmaceutical services (Web-based ordering, mail delivery), which could reduce total healthcare costs through greater efficiency
  - Consumer banking
- Helping disabled home-bound users to live fuller lives by enabling them to participate in healthcare, commerce, and social services without the need for in-person identity verification; and
- Improved online safety for minors.

IdM in the Context of National Security/Emergency Preparedness (NS/EP)

IdM has great potential to help fulfill national security, law enforcement, public safety, communications, security, and business and social needs. In addition, IdM advances are critical to NS/EP efforts because they help protect the networks, secure proprietary and Personally Identifiable Information (PII), and support Authentication assurance. Federal, State, and local governments rely heavily on digital communications for NS/EP purposes. Improved trust through development of a robust federation of interoperable IdM processes would enhance the ability of public officials to provide key NS/EP services.

For example, the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) use simple Personal Identification Number (PIN) based and subscription based access mechanisms to authenticate authorized users but these methods do not preclude unauthorized use of the system. As GETS and WPS transition to an open Internet or Internet-like environment, a higher level of assurance (for example, confidence in the identity of NS/EP users) would provide for protection against unauthorized use.

A number of key technical and policy capabilities to improve IdM for NS/EP communications include the development of a holistic IdM infrastructure, improved interoperability under a federated identity system, and the development of scalable and extendible technical architectures. [15]

IdM in the Context of Cybersecurity

IdM is one of the most critical foundations of cybersecurity. Without robust IdM capabilities, achieving cybersecurity goals will prove difficult.

IdM is one of the most critical foundations of cybersecurity. IdM vulnerabilities allow malicious actors to exploit networks and information. The current administration's commitment to broadening transparency across the Government will likely have cybersecurity implications and intensify the need for a federation of interoperable IdM processes. Without robust IdM capabilities, achieving cybersecurity goals will prove difficult. As the Federal centralized management of cybersecurity matures, solutions will emerge for integrating IdM within the communications and IT infrastructure in a way that balances security and privacy.

Problems and Impediments in the Current Operating Environment

Today's Internet originated in a closed environment in which a secure framework for managing identity was not required. As the Internet grew beyond its original closed environment, the need for a secure identity framework became more apparent. Existing identity credentials are weak and typically depend on both the context and application for which they were initially developed. In most cases, such identity credentials cannot be used in other situations or environments. For example, a patient may use a bank card to access funds at the bank or pay for a doctor visit, but the card cannot be used to verify the patient's insurance information. The lack of a uniform approach to establishing trust and confidence across different IdM federations impedes interoperability. The current dependence of identity assurance on the trust and confidence of a unique identity provider has played a large role in the maintenance of disparate IdM systems, effectively precluding interoperability.

Both the Government and the private sector have made significant progress in isolated areas of IdM. However, these positive efforts in Government and industry are not yet coordinated within an overarching strategic framework.

The successful development of a comprehensive interoperable IdM strategy requires overcoming cultural, technical, strategic, and economic problems. These problems extend to the Government, the private sector, and individuals. Both the Government and the private sector have made significant progress in isolated areas of IdM. However, these positive efforts in Government and industry are not yet coordinated

within an overarching framework. There are four areas of concern that must be addressed in pursuit of a comprehensive IdM strategy, specifically:

- Social factors;
- Commercial factors;
- Technological factors; and
- Government factors.

The social factors include the following:

- The socially-acceptable limits of Government-sponsored IdM activity have not been rigorously established, nor effectively validated with the private sector or the public. Absent defined limits, the Government risks pursuing technologically-attractive initiatives that may be socially undesirable.
- Cultural sensitivity to the prospect of a national identity card complicates the adoption of IdM processes and needs to be accommodated.
- Historically, both the private sector and the public have considered IdM technology processes to be intrusive. Before this resistance can be overcome, a comprehensive cost-benefit analysis in support of IdM system development and implementation must be conducted. First and foremost, the Government must offer the private sector and the public a trusted, easy-to-use, well-understood process that can protect privacy. Second, the Government must articulate the benefits that the IdM strategy can offer to the public, the private sector, and the Government, and make a convincing argument that a ubiquitous IdM infrastructure will be worthwhile.

The commercial factors include the following:

- Any broad federation of interoperable IdM processes must be sufficiently attractive to the general public (that is, these processes must be simple to use and understand). With these attributes, the private sector will be:
  - Encouraged to develop business applications that make deployment of the IdM capabilities economically feasible; and
  - Able to ensure public acceptance of processes involved and actions demanded of them. [16]
- Business cases must be developed that support emergence and sustainability of large-scale, commercial IdM processes; this has not yet been done.

Technical factors include the following:

- In today's environment, the lack of standards between independently-sponsored and managed IdM systems inhibits interoperability and extensibility.
- The various IdM federations do not share a uniform approach to establish trust and confidence across different IdM federations, including the vetting processes and identity validation.
- There are numerous Certificate Authorities; [17] in many cases, certificates do not interoperate with each other.

Government factors include the following:

- Government separates IdM programs designed to support security screening from those designed to facilitate the delivery of goods and services and access to information. This approach causes duplication of effort, inhibits efficient management, and artificially divides activities and applications across Government.
- The absence of a central IdM governance process across all Governmental IdM activities, including identity-sensitive [18] applications, inhibits Government's ability to holistically manage and advance IdM in support of the full range of security and efficiency drivers.

The Government can become the catalyst for addressing all of these factors and can ultimately implement a comprehensive, national IdM strategy.

Need for an Identity Strategy

Current Government and private sector IdM systems are numerous and stove-piped, causing redundancy and inefficient and uncoordinated IdM efforts. Private sector owners and operators of the Nation's information and communications technology (ICT) infrastructure, along with Government, have a vested interest in exploring potential solutions to reduce the frequency and impact of attacks on the Nation's network infrastructure and services, especially during emergency situations. The evolving and ubiquitous nature of the Internet demonstrates the criticality of ICT infrastructure to global security and stability.

A successful IdM strategy should promote a policy of interoperability and coordination among disparate systems to ensure both ease of use and security. If the private sector and Government develop a federation of interoperable IdM processes enhancing identity trust, awareness, and education among end users, providers, and devices, then the these strengthened network trust relationships will enhance the security posture of the United States.

A successful IdM strategy should promote a policy of interoperability and coordination of disparate systems to ensure both ease of use and security. If the private sector and Government develop a federation of interoperable IdM processes enhancing identity trust, awareness, and education among end users, providers and devices, then these strengthened network trust relationships will enhance the security posture of the United States. A comprehensive strategy and supporting federation of interoperable IdM processes would lead to more efficient use of Government and private sector resources, promote growth and innovation, and improve end user convenience when engaging in transactions across various domains. [19] Additionally, an effective, comprehensive IdM strategy will improve the management of PII and ensure the implementation of strict controls to protect unauthorized disclosure of privacy information across different domains. [20]

Currently, the international community is actively engaged in the debate on IdM. Specifically, digital identity is at the top of the Critical Information Infrastructure agenda of the European Union, with several member states pioneering projects and deployments in this area. The time is ripe for the United States to join the debate and leverage this opportunity to demonstrate leadership in the development of a unifying internationally interoperable solution.

Comprehensive IdM Strategy Characteristics and Principles

Given the factors described above, a comprehensive IdM strategy developed jointly by Government and the private sector could be the first step toward developing a federation of interoperable IdM processes. Today, the IdM space is fragmented, affecting the availability, reliability, and accuracy of its processes.

A comprehensive IdM strategy must address the following categories of Entities:

- **People.** IdM includes a definable set of persons, who by their nature, will be everything from Federal employees, entitlement beneficiaries and individual citizens; to prospective foreign visitors to the United States and visa recipients; to criminals, fugitives from justice, and subjects of intelligence or counter-intelligence interest."

- **Digital IT Devices, Network Components, and Services.** IdM necessarily embraces the digital IT devices, network components, and services upon which identity attribution is predicated and through which it is communicated, such that each of these are strongly individually identifiable.

- **Software Components.** Authentication of trusted software components, such as operating systems and communication software, are critical to maintaining the chain of trust.

- **Objects.** Beyond the humans whose identities must be verified, and the hardware and software elements supporting the identification and verification processes, inanimate objects may also be verified and tracked, including: (a) material and goods entering the United States via air, land, or

sea portal; (b) sensitive controllable objects used in commerce (such as pharmaceuticals or radioactive materials); and (c) digital rights or other objects of interest. This could extend to digital data and multimedia objects, including database records and documents.

Interoperability at the national and global level is critical to supporting multiple IdM solutions across communities and enables trust relationships within larger federations. The global information environment is the medium across which all identity-based transactions are conducted on network systems. Interoperability in physical access requires adoption of standardized credentials or other access protocols.

A verifiable Trust Anchor [21] methodology available to Government, the private sector, and social groups will create a mechanism all can use to issue authentic identities associated with a particular Trust Anchor. Essential Trust Anchor attributes include the abilities to trace:

- The asserted identity of some object or person back to the Trust Anchor; and
- The application to root sources and stores of digital identity data, both local and network-based.

Choice-based participation is crucial so that end users can decide whether or not to participate in the IdM federation and determine the degree of Authentication commensurate with the level of sensitivity of their transactions. In some cases, end user choice will be linked to specific identity-sensitive applications. If they anticipate some benefit to enrolling in such applications, individuals may be willing to provide certain, otherwise private, information as a condition of the enrollment process.

A successful federation of interoperable IdM processes would support an overarching, comprehensive IdM strategy with broad applications across a spectrum of communities and services and involve three key operational characteristics: (1) Interoperability; (2) Trust Anchors; and (3) Choice-based participation.

A comprehensive national IdM strategy must accommodate various levels of assurance to meet the diverse transaction needs. IdM must therefore provide a wide variety of enrollment options, identity data vetting/proofing capabilities, privacy protection capabilities, and Authentication mechanisms for nomadic users.

Additionally, a comprehensive national IdM strategy involves a key systemic characteristic—accountability—where all involved parties adhere to agreed-upon, standard procedures and processes, validated periodically with consistently applied rules (with appropriate consequences when users do not adhere to them). This ensures that all users respect the rules of the federation of interoperable IdM processes and diminishes the probability of exploitation of the system infrastructure.

Commercial IdM service providers exist today and will likely increase in number, expand their roles and offerings, and develop business opportunities to meet the growing national IdM need. The national IdM strategy must embrace commercial IdM service providers willing to collaborate with the Government to develop standards-based interoperability between Federal and commercial IdM processes.

A comprehensive IdM strategy should embody the following principles:

Privacy and Security

- Ensure security of process, data transmission, and storage;
- Ensure continuing emphasis on civil liberties and privacy;
- Provide secure management and use of PII and digital identities [22] where Government participation is non-intrusive, PII data storage is kept to a minimum, and disclosure of PII occurs only with the consent of the end user [23] (except where the Government, pursuant to appropriate legal process and other lawful circumstances, has the authority to access it);

- Provide safeguards against unauthorized and unintended use, aggregation, dissemination and transfer of information;
- Maintain a network of vetted digital-identity repositories as Trust Anchors to assert identities within the federation of interoperable IdM processes.
- Provide oversight of standards processes required to support all IdM functions (to include aspects of digital identities and their repositories, standardized applications interfaces to permit 'plug and play' fielding of new applications, and processes of the supporting IT infrastructure);
- Ensure that IdM processes are auditable, enabling complete, automatic, and secure record keeping where appropriate;
- Ensure Choice-based participation among all stakeholders that accommodates different social customs regarding privacy and anonymity; [24] and
- Ensure that the security capabilities of IdM processes are auditable. [25]

Education & Outreach

- Conduct broadly-based and sustained outreach and education activities to encourage societal engagement and frame the case for defined, measurable benefits, recognizable by participating organizations and private citizens;
- Create an international liaison and outreach programs to seek synergies and opportunities for alignment with similar efforts abroad;
- Demonstrate a benefit for all targeted stakeholders, including Government, the private sector, society, and individual end users; and
- Encourage significant investment by industry and Government to ensure that the infrastructure required for implementation is in place.

Availability

- Implement easy-to-use technology [26] and create incentives for users to adapt the technology;
- Function in broad terms so that the strategy can be adapted for use in many communities throughout the private, civil, and public sectors, and globally while using interoperable applications to ensure consistency and efficiency;
- Provide extensibility that enables various communities to tailor identity profile attributes;
- Ensure ubiquitous availability, at global distances, of strong verification of stored digital identity upon demand;
- Provide standards-based connectivity, interoperability, and extensibility of the supporting information technology (IT) architecture; and
- Enable prospective application sponsors to develop, install, and operate applications in a way that permits the supporting IT grid to be seen as a freely available, ubiquitous service.

Policy and technology development in support of the above principles will help drive the realization of a comprehensive national IdM strategy.

Activities within the Federal Government

The size and complexity of the total Federal IdM enterprise is considerable. The enterprise will be highly diverse in both organization and relevance. Management structures and approaches would be broadly-based and much consideration should be given beforehand to ensure the efficient formulation and execution of the IdM strategy.

The Federal Government has expended substantial effort to consolidate and coordinate IdM technologies and approaches among the departments and agencies. However, to ensure the mission and to best achieve a comprehensive IdM strategy, the Federal Government would require a single office, independent of other departments and agencies, to oversee, coordinate, and direct IdM efforts across the entire Executive Branch. The interagency mission would be to develop, enable, and implement identity-sensitive applications with cross-organizational interoperability, coordinate configuration and change management, develop and adopt standards, and develop consistent legal and policy approaches to IdM across the Federal Government in the performance of all its missions. This process would provide a horizontal integration and coordination of many preexisting authorities, charters, responsibilities, and programs across the Federal Government. Through this process, the Government would also interact with commercial identity-sensitive activities that require interoperability with Federal IdM processes.

It is possible that the organizational model of a National Coordination Office (NCO) may be attractive as the home of Federal IdM governance. Current examples of this include the NCO for Networking and Information Technology Research,* the NCO for Space-Based Positioning, Navigation and Timing,** and the National Nanotechnology Initiative.*** In all these cases, authorizing legislation has established a Federal charter and allocated funding. These organizations focus and direct the advancement of large-scale, broadly-impacting, and long-term technology issues of great national significance. This may be an effective way to achieve efficient and enduring management of IdM within Government, introduce the concept to the American public in optimal ways, and foster research into technologies. A successful IdM solution will operate on a global scale and support identity-sensitive applications to enhance the performance of Federal missions and citizen services.

* http://www.nitrd.gov
** http://www.pnt.gov
*** http://www.nano.gov

IdM Stakeholder Incentives

The development of a holistic, comprehensive IdM strategy could help coordinate efforts among the numerous private sector, Government, and individual stakeholders, while protecting and promoting their values and concerns, including:

- Secured communications for NS/EP needs;
- Increased security for online transactions and storage;
- Protection against fraud and identity theft; and
- Protection of privacy and civil liberties.

Private Sector and Individual User Incentives

Realistic potential exists for the private sector and individuals to benefit from participation in a federation of interoperable IdM processes. The current financial, political, and security environment provides a timely and unique opportunity to identify and prioritize critical IdM requirements. The shift towards digital communications, storage, and transactions in healthcare, banking, finance, commercial and retail activities, social networking, and print media has left individual end users increasingly at risk of identity theft, and private sector enterprises increasingly at risk of fraud in electronic commerce. Over the past 5 years, identity theft has emerged as the leading economic crime reported to the Federal Trade Commission Identity Theft Survey Report. [27] A robust federation of interoperable IdM processes would provide much-needed protection for consumers as digital communications supersede more traditional

methods of commerce. In addition, in the modern business environment where corporate data may be stored on third-party premises and employees are increasingly nomadic and require access from any location, the ability to provide the appropriate level of access has become a business necessity.

To motivate the private sector and individual end users to participate in a Choice-based IdM federation, the scheme must offer something these users value when requiring them to provide identity information for the sake of secure Authentication. The private sector and the general public will not accept solutions that degrade or diminish privacy by failing to adequately protect stored data. A federation of interoperable IdM processes would enable end users to assert their identities with confidence. [28] It is ultimately desirable that end users retain control over their information, but some organizations may need to have access to particular data for certain operations, such as human resources. Solutions that degrade trust or diminish privacy by failing to adequately protect stored data will not be accepted by the private sector and the general public.

Although high levels of privacy are crucial in certain cases such as healthcare and insurance, even in these areas some services will constitute a higher risk and value than others and should have access control mechanisms appropriate to those risks and values. In addition, a federation of interoperable IdM processes can include system maintenance of personal identity data that requires strong privacy protection; some users may expect to retain control over the use of at least some of this personal identity data, at least in some contexts.

Individual end users will not voluntarily participate in an IdM program if it is perceived to be inefficient, burdensome, risky, unreliable, or costly. A federation of interoperable IdM processes should offer a clear benefit to mission goals.

Individual end users will not voluntarily participate in an IdM program if they perceive it to be inefficient, burdensome, intrusive, costly, unreliable, or of dubious or minimal value. To ensure effective participation by all stakeholders, the comprehensive IdM vision and strategy should offer a clear benefit to their missions or business processes. A successful comprehensive IdM vision and strategy balances the private sectors' and individual end users' desire for privacy protection with the universal need for improved security; it must also take into account that privacy and security needs may vary under different situations. To help build confidence in the federation of interoperable IdM processes, the private sector could develop an insurance model in the event of an identity breach to help build confidence among private sector and civil society stakeholders. The Government can help communicate the benefits of IdM by devoting resources to strengthen the sharing of threat information.

A robust federation of interoperable IdM processes would provide much-needed protections for consumers as digital communications supersede more traditional methods of commerce.

In a Choice-based system, those who participate even minimally will be afforded a level of security they would not otherwise have, and their actions will also narrow the range of networks vulnerable to malicious actors. Private sector and individual end users will likely subscribe to an IdM solution if they feel the information they are providing online is protected. It is important for the Government to demonstrate the tangible security benefits of enhanced IdM capabilities while addressing privacy concerns and showing the other benefits IdM offers. [29] A federation of interoperable IdM processes that fails to provide significant security improvements and privacy protection will never gain the support of the private sector and individual end users.

U.S. Government Incentives

Across the board, the U.S. Government stands to benefit from strengthened accountability and Attribution through robust IdM. The United States increasingly relies upon ICT for communications, military operations, commercial transactions, and banking and financial transactions. The Government and the private sector currently collaborate on several IdM efforts. Joint partnerships may help to broaden

incentives for both sectors and improve efficiency. [30] Cost and liability risks must also be carefully examined in the context of a broad approach to an IdM strategy.

The lack of coordinated United States leadership in international IdM efforts, coupled with the absence of a comprehensive national IdM strategy, places telecommunications-related national security and economic equities at risk.

If the integrity of the infrastructure were compromised by intrusion and corruption, both economic and national security would be placed at risk. Specifically, exploitation of the Internet and other communications systems could lead to unauthorized disclosure of identity information and unauthorized access to Government systems with risks of disclosing sensitive, classified information.

The Government and the private sector could benefit by collaborating to develop a federation of interoperable IdM processes.

During emergencies, Federal, State, and local governments rely on the availability of trusted Internet and other communications systems. NS/EP users have the same characteristics as most IP network users—they are nomadic and demand access to all services at any time. However, they also differ from ordinary users as they need priority access to respond to events where lives and property are in imminent danger. Consequently, network operators and service providers must be able to verify the identity of NS/EP emergency responders. These providers need a mechanism to establish trust in an NS/EP environment, and IdM provides that mechanism. A lack of IdM capabilities could result in a situation where unauthorized users have access to NS/EP priority services, perhaps interfering with an emergency responder's ability to use those services to fulfill the mission. Consequently, it is in the Government's best interest to pursue the development of a federation of interoperable IdM processes. A strong IdM system, based on robust trust in the Internet infrastructure and design, increases consumer confidence and ensures the Government's ability to rely on the Internet and other communications systems for commercial activities and security operations.

Findings and Conclusions

The findings and conclusions in this section are derived from the above discussion and are presented here in direct support of the recommendations in Section X: Recommendations below.

Findings

Open and Secure Cyber Environment

- Based on the Identity Issues Task Force's examination of the IdM environment and previous reports, the Task Force believes that a robust identity strategy will provide a crucial underpinning for success in most wide-ranging cybersecurity initiatives. The Task Force also believes that the current political and policy landscape is ripe for promoting a comprehensive national strategy to ensure a trusted identification scheme for Entities (e.g., people, objects, devices, or organizations), coupled with Attribution [31] and Authentication assurance [32] requirements. Without such a strategy, malicious actors will continue to easily pose as legitimate users to exploit these networks and impact NS/EP capabilities and everyday business commerce.

- A comprehensive and sustained public outreach and education process will be necessary to support and nurture broad public acceptance of IdM. This process must emphasize the protection of the privacy rights of both the initiating and the receiving parties as a paramount objective.

- The administration's commitment to broadening transparency throughout Government will likely have cybersecurity implications and increase the need for an implementable federation of interoperable IdM processes

- High levels of privacy are crucial in certain cases such as healthcare and insurance; however, even in these areas, some services will constitute a

higher risk and value than others. Access control mechanisms should be available to accommodate the various levels of risks and values.

Global Interoperability

- The progress of national IdM in Government, business, and society will be commensurate with the extent to which it provides measurable and recognizable benefits to identity sponsors and end users. Therefore, identity-dependent applications should be encouraged to affiliate with an emergent national IdM process. At the same time, standards must be developed to support physical security applications within IdM processes.

- Global discovery and interoperability are essential to a successful federation of IdM processes and the need for U.S. engagement in various global forums is evident. The development of a national IdM strategy will help the Nation leverage its influence in international forums and promote the adoption of global, interoperable IdM standards in the best interests of the U.S. Government and private sector. Given the current international focus on IdM, the time is ripe for the United States to start influencing the debate.

- Despite laudable progress being made in many different areas across a broad organizational front, Government does not yet have a cohesive strategy to fulfill the potential of its considerable investment in all aspects of IdM, nor to meet the emergent need.

- The speed with which technology and media formats proliferate and expand contributes to evolving IdM challenges and the Government's stove-piped structural organization impedes internal interoperability.

- No uniformly-implemented approach exists to establish trust and confidence across different federations.

- There are inadequate drivers and incentives for uniform implementation to establish trust and confidence across different IdM federations.

- A federation of interoperable IdM processes, coupled with trust in the Internet infrastructure and design, would also increase consumer confidence and ensure the Government's ability to rely on digital communications systems for commercial activities and security operations.

- Individual end users will not voluntarily participate in an IdM program if it is perceived as inefficient, burdensome, intrusive, or costly.

Commerce

- Give the recent emphasis on efforts such as physical security screening, cybersecurity, healthcare technology innovation, and economic initiatives, consensus is emerging among key stakeholders in support of a broad IdM approach that covers a spectrum of issues, applications, and communities. This 'critical mass' is leading to greater awareness of IdM concerns and opportunities for IdM policy development and implementation.

- A comprehensive IdM strategy and supporting federation of interoperable IdM processes would enable more efficient use of Government and private sector resources, promote growth and innovation, and improve end user convenience when engaging in transactions across various domains. [33]

- Any broad interoperable IdM scheme must be sufficiently attractive to the general public (e.g., simple to use) to encourage development of interoperable IdM systems and business applications, thus making deployment of IdM capabilities economically attractive. [34] This will encourage the expanding role of commercial IdM service providers.

- It is important for a national IdM strategy to accommodate various levels of assurance to meet the diverse needs of the transactions being considered by both parties.

Conclusions

An Open and Secure Cyber Environment

- A strong degree of trust among all IdM stakeholders is crucial to the success of a federation of interoperable IdM processes.
- If IdM stakeholders do not address the fundamentals now, then more isolated IdM systems will emerge and it will become more difficult to adopt viable comprehensive and interoperable IdM solutions in the future.
- A federation of interoperable IdM processes should be voluntary and limit the amount of personal and proprietary information that is stored in a central location beyond the identity owner's control.
- Prior to implementation, the national IdM strategy security benefits—enhanced IdM security, personal convenience, expanded functionality, and improved organizational efficiency—must outweigh the costs, inconvenience, and privacy concerns. [35]
- The relationship between IdM efforts and cybersecurity will benefit from further exploration as the Federal centralized management of cybersecurity matures.
- Over time, as Federal organizational and programmatic approaches to cybersecurity mature, it will become increasingly important to identify the specific gaps and overlaps in policy and technology in the total relationship between cybersecurity and IdM.

Global Interoperability

- The United States must align domestic efforts with the ongoing work of the international community (e.g., standards bodies and foreign governments) and work with all stakeholders to ensure international interoperability.
- The national IdM need requires a network of interoperable, federated digital identity repositories. These will collectively support the establishment of Trust Anchors to confidently provide identity validation authority to support all needs.
- The Government should initiate a public-private partnership to help define the IdM space and work toward developing a federation of interoperable IdM processes that includes identity verification and validation, and Authentication of users, devices, objects and information under differing circumstances (e.g., general Web services, financial transactions, healthcare/insurance, and personal data access).
- A successful federation of interoperable IdM processes supports an overarching, comprehensive strategy with broad applications across a spectrum of communities and involves three characteristics: (1) interoperability; (2) Trust Anchors; and (3) Choice-based participation.
- A national IdM strategy will require a comprehensive governance process, embracing the full scope and scale of IdM as described in this report.

Commerce

- A federation of interoperable IdM processes must demonstrate economic incentives/viability to ensure commercial participation and interoperability of identity service providers, private sector buy-in, privacy protections to ensure individual end user buy-in, and ease-of-use for general adoption.
- Industry and public acceptance are at the core of any progress in a federated IdM, as extended beyond the Government itself. This collaboration should involve a multi-faceted and sustained program of outreach, education, partnership, and incentives.
- Any emergent national IdM strategy must recognize and embrace the roles and participation of commercial IdM service providers of all types. Service providers should be invited to partner with Government to create an interoperable, standards-based IdM environment that can be extended to support all public and private IdM needs.

- A federation of interoperable IdM processes should leverage current and future Government and private sector investments, R&D, and Government agenda items to promote widespread adoption.

- A comprehensive IdM strategy should incorporate the key principles described in Section VII.

Government can help communicate the benefits of IdM by devoting resources and shoring up infrastructure and networks to protect NS/EP equities. In a recent letter [36] to the President in response to questions posed by his staff, the NSTAC offered prioritized recommendations regarding the greatest needs for cybersecurity at the national level. Those recommendations were based on historic reports and analyses conducted by the NSTAC in recent years. The first five of the eight stated priorities were:

- Adaptation of the current Federal Government organizational authorities for IdM to meet the desired need and optimize results;

- Information sharing;

- Identity Management;

- Standards; and

- Legal considerations.

The NSTAC finds that current IdM requirements encompass these priorities within a single, holistic vision. Both the Government and the private sector have performed great work contributing to IdM goals and objectives. Service-specific systems and methods for retail, enterprise, communications, and other business applications proliferated with the growth of the Internet and IP-based technologies. However individually beneficial these are, these activities do not rise to the level of the coordination, efficiency, and scope of vision required for a holistic, integrated, national IdM strategy.

In light of these circumstances, the NSTAC concludes that the Government, working collaboratively with the private sector, the public, and interested nations, should develop a comprehensive national IdM vision and strategy that meets the security, business, and personal needs of American society and addresses the organizational, programmatic, legislative, and cultural components of IdM.

All four components of the total strategy listed below should be embraced and advanced collectively to achieve needed IdM alignment, effective collaboration between Government and industry, and broad social engagement. Taken together, these efforts will provide the presidential emphasis, streamlined authorities, and broad engagement needed to achieve the beneficial effects of IdM across the Nation.

National Integrated and Holistic IdM Vision and Strategy

Organizational

- Government Lead/Governance Process
  - Public/Private Collaboration
  - Accountable organization and individual
  - Federated IdM
- Centralized Authority
  - Budget Control
  - Resources
  - Program Charters
  - Coordination and movement toward a strategic goal

Programmatic

- Standards and Practices Collaboration
- Public/Private Collaboration on R&D
- Applications/Appropriations
- Embed IdM Solutions with:
  - Cybersecurity
  - Healthcare
  - Other Broad Scope Initiatives

Policy and Legislative

- Policy and Legislative Actions as Needed
  - Cybersecurity
  - Public/Private Partnerships
  - Funding
  - Authorities
  - Legislative Review
  - Consolidate Currently Dispersed Responsibilities
  - Rationalize
  - Integrated Oversight

Cultural

- Education
- Communications Initiatives
- Privacy Concerns
- Civil Liberties Concerns
- Outreach
- Communication Plan –
  - President Must Sell Vision

Recommendations

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions:*

1. ***Demonstrate personal national leadership in IdM to positively influence the national culture, attitude, and opinion toward IdM.*** Successful development and implementation of a national IdM vision and strategy requires national commitment across Government, industry, and individuals dependent on cyber applications

2. ***Charter a national IdM office under specifically appointed and dedicated leadership, in the Executive Office of the President.*** This office must have powers to integrate and harmonize national IdM policies and processes, including those related to law enforcement and security, as well as physical and logical access controls. This office should seek active private sector participation in developing such policies and processes in order to succeed and to ensure that successful solutions are shared with the private sector, as appropriate.

3. ***Direct the newly created office to develop a coordinated programmatic agenda to implement a comprehensive IdM vision and strategy to address, at a minimum, four component areas, specifically: Government organization and coordination; public-private IdM programs; policy and legislative coordination; and national privacy and civil liberties culture.*** Because no existing Government office or organization is engaged in all areas and issues across the total scope of IdM, new approaches are required to harness the expertise and interests across all areas.

   With respect to Governmental organization and coordination, establish a single, authoritative and comprehensive IdM governance process with a dedicated mission and office under an accountable official reporting directly to the President, embracing all Federal policy, technology, and IdM application activities related to both screening and access controls. The established lead official should have control over defined IdM programs and resources across Government, including budget, as needed to advance Federal IdM under a single coherent strategy.

   With respect to public-private programs, direct the appropriate Federal Government departments and agencies to work with the private sector to develop and advance a comprehensive and progressive IdM Research and Development agenda, focusing on Government-civil IdM interoperability. This effort should seek to establish interface standards to enable IdM applications to access and securely operate on global communications networks. In addition, this effort should partner with industry to embed IdM solutions in identity-sensitive applications of all kinds, promoting standards-based public-private programmatic collaboration.

With respect to policy and legislative coordination, determine what changes to policy and regulation should be made, and what legislative initiatives should be advocated to move quickly toward national IdM goals. Further, establish policy and a legal framework to support internal Federal activities and streamline Government-civil collaboration and partnership in support of those goals. In particular, the IdM office should pursue legislative efforts to support National IdM governance, organization and authority needs, as appropriate.

With respect to national privacy and civil liberties culture, develop a comprehensive and sustained communications plan to promote IdM reflecting key national and social values and embracing the strong National conviction to protect privacy and civil rights of both initiating and receiving parties as the national IdM strategy is developed and implemented.

All four of these components must be acted upon to achieve needed IdM alignment within Government, and between Government and industry. Collectively, these efforts will provide the Presidential emphasis, streamlined authorities, and broad engagement needed to achieve the beneficial effects of IdM throughout the Nation.

Footnotes

1 "Banks Test 'Text Messaging' Security" Investor's Business Daily (08/10/07) P. A4 ; Howell, Donna
Banks and brokerages have been on the hunt for just the right balance between convenience and cost to boost log-on and transaction security for customers. Tokens have been one solution to reinforcing banking security, as users type an up-to-the-minute passcode that is displayed on a token. Thieves' efforts are thus thwarted from logging on as a user, even if they know the user's name and password. Financial firms are also considering sending users a one-time pass code via text messages to their mobile phones, or by an automated phone call that would eliminate the use for tokens. Passcode generators can also be built into cell phone handsets. Since most consumers have cell phones, sending mobile notifications could be a viable authentication measure. A built-in credit card authentication option is also being considered by financial institutions. The card would display a one-time passcode once a pressure-sensitive area of the card is touched. VeriSign's Fran Rosch says this technology will undergo pilot tests and reach a sizeable distribution by next year.

2 "Information Technology Progress Impact Task Force Report on Convergence," *President's National Security Telecommunications Advisory Committee (NSTAC).* May 2000. http://www.ncs.gov/nstac/reports/2000/Convergence-Final.pdf.

3 For the purposes of this report, Identity Management (IdM) is the structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use, and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices *(T SG17 Q6 Identity CG. International Telecommunication Union [ITU]).*

4 For the purposes of this report, the term 'networks' includes Internet Protocol (IP)-based networks, digital communications, and all telecommunications network systems. Please see Appendix F for the definition of *Internet.*

5 Various sources cite current cyber incident information and statistics, including us-cert.gov, sans.org, govtech.com, and cert.org.

6 For the purposes of this report, *Authentication* is the provision of assurance of the claimed identity of an entity.

7 *National Science and Technology Council,* Identity Management Task Force Report-2008, www.ostp.gov

8 *Center for Strategic & International Studies,* Securing Cyberspace for the 44th Presidency, 2008, www.csis.org

9 Going beyond securing communications networks and commerce, IdM could be used to help enforce immigration laws and improve border security, without adversely impacting lawful residents.

10 The White House Agenda. http://www.whitehouse.gov/agenda/.

11 The President's National Security Telecommunications Advisory Committee, "Vulnerabilities Task Force Report on Trusted Access," January 27, 2003.

12 For the purposes of this report, Attribution is the association of descriptive information bound to an entity that specifies a characteristic of an entity (such as condition, quality or other information associated with that entity) to that particular entity (NSTAC 2009).

13 Rutkowski, Anthony, December 2008, "A Global Perspective on Identity Issues."

14 Choice-based participation is crucial so that end user have a clear choice in whether or not to participate in the IdM federation and in determining the degree of Authentication commensurate with the level of sensitivity of their transactions. In some cases, end user choice will be linked to particular identity-sensitive applications. Applicants may be willing to voluntarily enroll in such applications, and provide certain, otherwise private, information as a condition of the enrollment process, if they expect to realize some benefit in doing so.

15 2008 Research and Development Exchange Workshop Proceedings, September 2008, "Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment."

16 *Ibid.*

17 "NSTAC Report to the President on Physical Assurance of the Core Network", FOUO, dated November 6, 2008. Certification Authority Services: Services infrastructure and facilities involved in providing identity management and chain of trust validation for critical Internet services and transactions."

18 An application wherein accesses and privileges of an individual, organization or group are variable, depending on their identity attributes.

19 "The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers – Volunteer Group Draft," Organization for Economic Cooperation and Development (OECD). 27 January 2009.

20 NSTC Subcommittee on Biometrics and Identity Management, September 2008, "Identity Management Task Force Report 2008."

21 For the purposes of this report, a Trust Anchor is defined as an authoritative entity that has responsibility over verifying an identity.

22 NSTC Subcommittee on Biometrics and Identity Management, September 2008, "Identity Management Task Force Report 2008."

23 Microsoft-Scott Charney, 2008, "Establishing End to End Trust."

24 *Ibid.*

25 *Ibid.*

26 Excerpts adapted from the 2008 Research and Development Exchange Workshop Proceedings, September 2008, *"Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment."*

27 Federal Trade Commission. "Identity Theft Survey Report," Prepared by Synovate. September 2003. http://www.ftc.gov/os/2003/09/synovatereport.pdf.

28 Microsoft-Scott Charney, 2008, "Establishing End to End Trust."

29 *The ID Divide: Addressing the Challenges of Identification and Authentication in American Society.* June 2008. (Swire and Butts).

30 For lower levels of authentication, the Government currently partners with higher education entities and the Liberty Alliance, a group of private sector companies which works to develop open standard-based specifications for federated IdM and global identity theft prevention solutions, among other identity solutions, [www.projectliberty.org/liberty/about]. Management Board member organizations include: (1) America Online; (2) BT; (3) CA; (4) Fidelity Investments; (5) Intel; (6) Internet Society; (7) Novell; (8) NTT; (9) Oracle; and (10) Sun Microsystems. For lower levels of authentication, the Government current works within the Federal Bridge to collaborate with the private sector. [Spencer, Judith. "Identity, Credential and Access Management: The Government-wide Initiative," General Services Administration.]

31 See Appendix F for definition.

32 *Ibid.*

33 "The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers – Volunteer Group Draft," Organization for Economic Cooperation and Development (OECD). 27 January 2009.

34 Knode, Ron. "Identity Issues Report Precis: Digital Identity and Identity Management," 4 February 2009.

35 *The ID Divide: Addressing the Challenges of Identification and Authentication in American Society.* June 2008. (Swire and Butts).

36 Muller, Edward A. Letter dated 12 March 2009.

Participant List

Task Force Members

Computer Sciences Corporation
Mr. Guy Copeland, Co-Chair

Nortel Networks Corporation
Dr. Jack Edwards, Co-Chair

AT&T, Incorporated
Ms. Julie Thomas
Ms. Rosemary Leffler

VeriSign, Incorporated
Mr. Larry Schaeffer

Boeing Company
Mr. Bob Steele

Juniper Networks, Incorporated
Mr. Robert B. Dix, Jr.

Microsoft Corporation
Ms. Cheri McGuire

Qwest Communications International, Incorporated
Ms. Kathryn Condello
Mr. Andrew White

Raytheon Company
Mr. Frank Newell

Science Applications International Corporation
Mr. Henry Kluepfel

Telcordia Technologies, Incorporated
Ms. Louise Tucker

VeriSign, Incorporated
Mr. William Gravell

Verizon Communications, Incorporated
Mr. Marcus Sachs

Other Participants

ARTEL, Incorporated
Mr. Julian Minard

AT&T, Incorporated
Mr. Brian Daly
Mr. Martin Dolly

Bank of America Corporation
Mr. Manoj Govindan
Mr. Todd Inskeep

Computer Sciences Corporation
Mr. Ron Knode
Mr. Jim Zok

ID Analytics, Incorporated
Mr. Tom Oscherwitz

Industry Canada
Mr. Bob Leafloor

Microsoft Corporation
Mr. Matt Broda
Mr. Phil Reitinger

Netmagic Associates
Mr. Tony Rutkowski

Nortel Networks Corporation
Mr. Abbie Barbir
Mr. John Yoakum

Raytheon Company
Mr. Clifton H. Poole

Telcordia Technologies, Incorporated
Mr. Robert Lesnewich
Mr. Ray Singh

Unisys
Mr. Mark Cohn

Verizon Communications, Incorporated
Ms. Deborah Blanchard
Mr. Russel Weiser

U.S. Government Personnel

Department of Commerce
Mr. William C. Barker
Ms. Tanya Brewer
Ms. Donna Dodson
Dr. Elaine Newton

Department of Defense
Mr. Dick Brackney
LTC Susan Camoroda, US Army
Mr. David Milhelcic

Department of Homeland Security
Ms. Sue Daage

Department of State
Mr. James G. Ennis

Executive Office of the President
Ms. Carol Bales
Mr. Duane Blackburn
Mr. Thomas Donahue

Federal Communications Commission
Mr. Pat Amodio

General Services Administration
Ms. Judith Spencer

Office of the Director of National Intelligence
Mr. Thomas Seivert

References and Bibliography

References

Howell, Donna. "Banks Test 'Text Messaging' Security" Investor's Business Daily (08/10/07) P. A4;

President's National Security Telecommunications Advisory Committee (NSTAC). *Information Technology Progress Impact Task Force Report on Convergence,* May 2000. http://www.ncs.gov/nstac/reports/2000/Convergence-Final.pdf.

Center for Strategic & International Studies, *Securing Cyberspace for the 44th Presidency,* 2008, www.csis.org.

http://www.nano.gov

http://www.nitrd.gov

http://www.pnt.gov

Muller, Edward A. Letter dated 12 March 2009 to Ms. Melissa Hathaway regarding the Nation's 60-day Cyber Review.

The ID Divide: Addressing the Challenges of Identification and Authentication in American Society. June 2008. (Swire and Butts).

The President's National Security Telecommunications Advisory Committee (NSTAC). *Vulnerabilities Task Force Report Trusted Access,* January 27, 2003.

Bibliography

Ahamad, Mustaque, Dave Amster, et al. *Emerging Cyber Threats Report for 2009: Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond,* October 15, 2008. Georgia Tech Information Security Center.

Albanesius, Chloe. *RIAA Confirms It Will Take Piracy Fight to ISPs.* December 19, 2008.

ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel (IDSP). *Final Report and Report Summary.* January 2008

Benson, Matthew. *Napolitano: Real ID a no-go in Arizona.* The Arizona Republic. June 18, 2008. http://www.azcentral.com/news/articles/2008/06/18/20080618real-id0618.html.

Carlton, Dennis, Peter Graham, and John Reiners. *Resolving the 'privacy paradox': Practical Strategies for Government Identity Management Programs.* November 2008. *IBM Institute for Business Value.*

Center for American Progress. *The ID Divide-Addressing the Challenges of Identification and Authentication in American Society.* June 2008.

Crosby, Sir James. *Challenges and Opportunities in Identity Assurance.* March 2008.

CSC Leading Edge Forum – Soren Thygesen Gjesse. *Architecture Blueprint for Leveraging Identity Federation.* Undated.

CSC Leading Edge Forum. *Digital Trust – Identity Management – Digitizing Your DNA.* Volume 2. 2007.

Document Security Alliance. *An Analysis of National Document Security Vulnerability.* March 2009.

ENISA Quarterly Review. Vol. 4, No. 4, October – December 2008.

Kartz, Black and Ryan. *Identity Management Reference Architecture Practicum Report.* FEAC Winter 2008 session, March 2008.

Federal Trade Commission. *Identity Theft Survey Report.* Prepared by Synovate. September 2003. http://www.ftc.gov/os/2003/09/synovatereport.pdf.

International Telecommunication Union (ITU) Standardization Sector – VeriSign. *A Trusted Provider Identity Framework for NGNs.* January 2009.

Knode, Ron. *Identity Issues Report Precis: Digital Identity and Identity Management.* 4 February 2009.

Langevin, McCaul, Charney, Raduege, et al. *Securing Cyberspace for the 44th Presidency.* 2008. Center for Strategic and International Studies.

McCallister, Erika, Tim Grance and Karen Scarfone. National Institute of Standards and Technology (NIST). Draft Special Publication 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* January 2009.

Microsoft-Scott Charney. *Establishing End to End Trust.* 2008.

National Security Presidential Directive – 59/Homeland Security Presidential Directive – 24. *Biometrics for Identification and Screening to Enhance National Security.* June 5, 2008. http://www.fas.org/irp/offdocs/nspd/nspd-59.html.

NSTC Subcommittee on Biometrics and Identity Management. *Identity Management Task Force Report 2008.* September 2008.

NSTAC Information Technology Progress Impact Task Force. *Information Technology Progress Impact Task Force Report on Convergence.* May 2000.

Presidents Identity Theft Task Force. *Combating Identity Theft-A Strategic Plan.* April 2007.

Rutkowski, Anthony. *A Global Perspective on Identity Issues.* December 2008.

Rutkowski, Anthony. I*dentity Management and Network Cybersecurity Forensics.* January 10, 2009

Rutkowski, Anthony. *Identity Management: exercise of FCC Authority.* January 2009.

Rutkowski, Anthony. *Survey of Network Forensics Exchange Initiatives.* January 2009.

Rutkowski, Anthony. *The Death of Paid Standards (and the Birth of New Identity Services).* February 2009.

Scholl, Matthew, Kevin Stine, et al. National Institute for Standards and Technology (NIST). *Draft Security Architecture Design Process for Health Information Exchanges (HIEs).* January 2009.

Organization for Economic Cooperation and Development (OECD). *The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers – Volunteer Group Draft.* 27 January 2009.

Silver, Dave, et al. (editors). General Services Administration. *Technical Approach for the Authentication Service Component.* May 4, 2007.

The UK Office of Public Sector Information. *Challenges and Opportunities in Identity Assurance.* March 2008. www.hm-treasury.gov.uk/d/identity_assurance060308.pdf.

The White House Agenda. http://www.whitehouse.gov/agenda.

2008 Research and Development Exchange Workshop Proceedings. *Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment.* September 2008.

Definitions

Definitions

These terms and definitions are drawn from many sources. In some cases, a term may have several definitions because it is used by different entities to describe various types of activity. With modern technology, and ICT in particular, it is sometimes difficult to find a word or phrase that accurately describes the activity. Understanding is helped by providing additional information about the situation or context in which the term is being used; this will be found in the notes column. In some cases, it helps to state the situation or context that does *not* apply.

Where a suitable definition exists for a listed term, the construction of new descriptions should be avoided. Ideally, a single definition should be agreed for each term; some are more difficult than others, but those agreed so far are shown in ***bold italics.***

All of the information contained below has been obtained from publicly available sources, primarily web-sites, and is not thought to have breached any Intellectual Property Rights or copyright.

Term	Definition	Source
Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.	ITU-T X.800
Anonymity	a. ***Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behavior such as user location, frequency of a service usage, and so on.***	ITU-T X.1121 (04), 3.2.1
	b. Lack of any capability to ascertain identity.	ITU-T Y.IDMsec
	c. The quality or state of being anonymous which is the condition of having a name or identity that is unknown or concealed.	OASIS SAML 2.0, RFC2828
Asserting Identity	An entity making an identity representation or claim to a relying party within some request context.	ITU-T IdM Editors
Assurance	A measure of confidence that the security features and architecture of the Identity Management capabilities accurately mediate and enforce the security policies understood between the Relying Party and the identity provider.	ITU-T Y.IDMsec
Attribute	***Note:*** *The FG IdM Framework document will discuss attributes in context with the significant technical implications that arise.*	
	a. Descriptive information bound to an entity that specifies a characteristic of an entity such as condition, quality or other information associated with that entity	ETSI TS102 042 V1.2.4 and ITU-T Y.IDMsec
	b. Information of a particular type. In IdM, objects and object classes are composed of attributes	ITU-T X.501
	c. A distinct characteristic of an object. An object's attributes are said to describe the object. Objects' attributes are often specified in terms of their physical traits, such as size, shape, weight, and color, for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, and network address.	WSIA Glossary

Term	Definition	Source
Authenticated Identity	A distinguishing identifier of a principal that has been assured through authentication.	ITU-T Y.2702, X.811
Authentication	The provision of assurance of the claimed identity of an entity.	ITU-T Y.2702, X. 811
Authorization	The granting of rights, which includes the granting of access based on access rights.	ITU-T Y.IdMsec, X.800
Biometrics	The use of measurable biological characteristics, such as fingerprint recognition, voice recognition, retina and iris scans to provide authentication.	BT Report on Identity Theft
Choice-based	Case in which end users have a clear choice in whether to participate in an IdM federation and over the degree of Authentication reflecting the level of sensitivity of their transaction.	NSTAC Identity Issues Task Force, 2009
Claim	***Note:*** *A Claim could just convey an identifier Another Claim might assert that a Digital Subject knows a given key. A set of Claims might convey personally identifying information. A claim might simply propose that a Digital Subject is part of a certain group. A claim might state that a Digital Subject has a certain capability. Claims may or may not be directed to specific Parties. A Claim is an association between a Claimant, a Digital Subject, and an Identity Attribute.*	
	An assertion made by a Claimant of the value or values of one or more Identity Attributes of a Digital Subject, typically an assertion which is disputed or in doubt.	Identity Gang
Credential	a. ***An identifiable object that can be used to authenticate the claimant is what it claims to be and authorize the claimant's access rights.***	
	b. Data that is transferred to establish the claimed identity of any entity.	
	c. The private part of a paired Identity assertion (user-id is usually the public part). The thing(s) that an entity relies upon in an assertion at any particular time, usually to authenticate a claimed identity. Credentials can change over time and may be revoked. Examples include; a signature, a password, a drivers license number (not the card itself), an ATM card number (not the card itself), data stored on a smart-card (not the card itself), a digital certificate, a biometric template.	
Digital Identity	a. ***The digital representation of the information known about a specific individual, group, or organization.***	Based on CERIAS
	b. A digital representation of a set of claims made by one party about itself or another digital subject.	Identity Gang, et al.
	c. A set of claims made by one digital subject about itself or another digital subject.	Cameron, CERIAS

Term	Definition	Source
Entity	***Note:*** *The choice was made to provisionally keep this definition open to any type of person (including legal persons, to facilitate e.g., eProcurement), but also to any other type of entity, such as objects (e.g., computers or other forms of machinery), digital resources or processes (e.g., programs), as this allows abstraction to the largest common element and thus offers the largest number of applications. In order for its existence to be acknowledged, an entity needs to have at least one unique identity. In an identity system implementation an Entity is abstract, conceptual, and non-modeled.*	
	a. ***Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.***	ITU-T Y.IdMsec
	b. An entity is anyone (natural or legal person) or anything that shall be characterized through the measurement of its attributes.	Modinis
	c. A person, physical object, animal, or judicial entity.	Identity Gang
	d. A particular thing, such as a person, place, process, object, concept, association, or event.	IEC 61804-2, ed. 2.0
Federation	a. ***An act of establishing a relationship between two or more entities or an association compromising any number of service providers and identity providers.***	Based on ETSI TR 133 980 V7.5.0
	b. An established relationship among a domain of a single service provider or among next generation network providers.	ITU-T Y.IdMsec
	c. A federation is a collection of realms that have established a producer-consumer relationship whereby one realm can provide authorized access to a resource it manages based on an identity, and possibly associated attributes, that are asserted in another realm. A federation requires trust such that a Relying Party can make a well-informed access control decision based on the credibility of identity and attribute data that is vouched for by another realm.	FG IdM Use Case Working Group
Federated Identity	a. ***A collective term describing agreements standards and technologies that make identity and entitlements portable across autonomous domains.***	The Burton Group
	b. A single user identity that can be used to access a group of services or applications that are bounded by the ties and conditions of a federation.	ITU-T Y.IdMsec
	c. A shared identity and/or authentication, as the result of federation by either the Entity or by two or more organizations.	Identity Dictionary

Term	Definition	Source
Identifier	***Note:*** *In the context of IdM, identifiers are generally labels issued by some kind of authority or service provider, or established between peers. Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties.)*	
	a. ***An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/ applications, or other entities (e.g., physical or logical objects).***	ITU-T Y.2091
	b. A data object (for example, a string) mapped to a system entity that uniquely refers to the system entity. A system entity may have multiple distinct identifiers referring to it. An identifier is essentially a "distinguished attribute" of an entity.	OASIS SAML 2.0
	c. Either an "http" or "https" URI, (commonly referred to as a "URL" within this document), or an XRI (Reed, D. and D. McAlpin, "Extensible Resource Identifier (XRI) Syntax V2.0,".)	OpenID
Identity	***Note:*** *In the case of a person, the collection of attributes that make up their electronic/digital identity does not normally mean that the individual can be positively identified.*	
	a. ***Structured representations of an entity in the form of one or more credentials, identifiers, attributes, or patterns in a relevant context. Such representations can take any physical or electro-optical (digital or analog) form or syntax, and may have associated implicit or explicit time-stamp and location specifications.***	ITU-T SG17 Q6 Identity CG
	b. The properties of an entity that allows it to be distinguished from other entities.	The Digital Identity Glossary by P.T. Ong
	c. The attributes by which an entity is described, recognized or known.	ITU-T Y.IdMsec
	d. The essence of an entity and often described by its characteristics.	Liberty Alliance
	e. The essence of an entity [Merriam]. One's identty is often described by one's characteristics, among which may be any number of identifiers.	OASIS SAML 2.0
	f. The fundamental concept of uniquely identifying an object (person, computer, etc.) within a context. That context might be local (within a department), corporate (within an enterprise), national (within the bounds of a country), global (all such object instances on the planet), and possibly universal (extensible to environments not yet known). Many identities exist for local, corporate, and national domains. Some globally unique identifiers exist for technical environments, often computer-generated.	Open Group
	g. A collection of attributes which helps to distinguish one entity from another.	The Information Assurance Advisory Council (IAAC)

Term	Definition	Source
Identity Information	All the information identifying a user, including trusted (network generated) and/or untrusted (user generated) addresses. Identity information shall take the form of either a SIP URI (see RFC 2396) or a "tel" URI (see RFC 3966).	ETSI TS 183 007 V1.1.1
Identity Layer	***Note:*** *An identity layer attempts to develop convergence and interoperability regarding identity, can draw from multiple data stores, selectively exposing, or concealing data and attributes, according to policy*	
	Information can be exchanged between different systems.	FG IdM
Identity Management	The structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices.	T SG17 Q6 Identity CG
Identity Provider	a. ***An entity that creates, maintains, and manages trusted identity information for entities. An Identity Provider may include a Trusted Third Party as well as Relying Parties and entities themselves in different contexts.***	ITU-T IdM Editors
	b. A type of service provider that creates, maintains, and manages identity information for users/devices and provides user/device authentication.	ITU-T Y.IdMsec
	c. A service provider that authenticates a user and that creates, maintains, and manages identity information for users and asserts user authentication and other identity related information to other trusted service providers.	ITU-T Y.IdMsec
	d. An entity in an AAI that performs Identity Management.	TF-AACE
	e. Kind of service provider that creates, maintains, and manages identity information for principals and provides authentication to other service providers within a federation, such as with web browser profiles.	OASIS SAML 2.0
Internationalization	***Note:*** *The internationalization process is sometimes called translation or localization enablement.*	
	The process of planning and implementing Identity Management specifications, products, services, and administrative implementations so that they can easily be adapted to specific local technical platforms, languages, and cultures, a process called localization.	FG IdM
Internet	***Note:*** *The Internet originally served to interconnect laboratories engaged in Government research, and has now been expanded to serve millions of users and a multitude of purposes, such as interpersonal messaging, computer conferences, file transfer, and consulting of files containing documents.*	
	a. A worldwide interconnection of individual networks a) with an agreement on how to talk to each other, and b) operated by Government, industry, academia, and private parties.	http://www.atis.org/glossary/definition.aspx?id=4286
	b. The international computer network of both federal and nonfederal interoperable packet switched data networks. [47 USC 230]	

Term	Definition	Source
Interoperability	***Note:*** *Identifiers assigned in one context may be encountered, and may be re-used, in another place or time without consulting the assigner. Assumptions made on assignment may not be known to someone else.*	
	The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together to mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility of use in services outside the direct control of the issuing assigner.	ISO TC46/SC9 Identifier Interoperability WG
Object	***Note:*** *DOI = Digital Object Identifier*	
	A well-defined piece of information, definition, or specification which requires a name in order to identify its use in an instance of communication and identity management processing. Entity within the scope of the DOI system; the entity may be abstract, physical or digital, as any of these forms of entity may be of relevance in content management (e.g. people, resources, agreements).	ITU-T X.680 and ISO Project 26324
Owner	***Note:*** *An entity owns an identity (and therefore its access rights) due solely to the ability to authenticate it.*	
	The registered entity for an identity.	Identity Dictionary
Personally Identifiable Information (PII)	***Note:*** *See privacy.*	
	a. The information pertaining to any person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person). Note: Information that can be used to identify an individual should be defined by national legislation.	X.rfpg
	b. Any information that identifies a person to any degree.	PRIME
Privacy	***Note:*** *Privacy is a legal requirement which is divided into 3 areas: (1) User privacy andpreventing unwanted intrusions; (2) User privacy and CPNI protection; and (3) User privacy and anonymity. The nature an d exercise of the legislation vary in different jurisdictions.*	
	a. ***The right of entities to control or influence what information related to them may be collected and stored also by whom and to whom that information may be disclosed.***	ITU-T Y.IdMsec, X.800
	b. Ensuring that information about a person is protected in accordance with national, regional, or global regulations. Such information may be contained within a message, but may also be inferred from patterns of communication; e.g. when communications happen, the types of resource accessed the parties with whom communication occurs, etc.	Based on W3C Glossary
	c. A right to control the dissemination of the attributes of an entity.	Identity Dictionary
	d. The rights and limitations of access to and processing of personal data.	OMA
	e. Proper handling of personal information throughout its life cycle, consistent with the preferences of the subject.	Liberty Alliance

Term	Definition	Source
Revocation	The act (by someone having the authority) of annulling something previously done.	ITU-T Y.2701
Trust	***Note:*** *The risk/trust relationship depends on who you are and what you want to d o at any instance. The degrees of separation between parties can decrease the trust (increase the risk). The level of trust is typically based on the technical strength of the identity, but it also includes the evaluating entity's subjective considerations (e.g. feelings) of the reliability of the entity the identity represents. Trust is at least partially transitive (as in the case of notaries).*	
	a. A measure of reliance on the character, ability, strength, or truth of someone or something.	ITU-T IdM Editors
	b. Confidence that an entity will behave in a particular way with respect to certain activities (entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.)	FG IdM based on ITU-T Y.2701
	c. A reasonable level of confidence that an entity will behave in a certain manner in a given context.	ITU-T Y.IdMsec
	d. A subjective assessment. An instance of a relationship between two or more entities, in which an entity assumes that another entity will act as authorized/expected.	Identity Dictionary
	e. Trust is an evaluation, by an entity, of the reliability of an identity when the identity is involved in interactions.	Oughome
User	***Note:*** *A user may have several identities / usernames / user-ids / logon-ids / sign-ons.*	
	a. ***Includes end user, person, subscriber, system, equipment, terminal (e.g. FAX, PC), (functional) entity, process, application, provider, or corporate network.***	ITU-T Y.2701 Y.2091
	b. An identity where the identifier of the identity is the public part of a paired Identity assertion.	Identity Dictionary
Verification	The process of confirming a claimed Identity. For example; any one-to-one precise matching of an identity's registered credentials, such as in a logon or any non-AFIS process. Usually performed in real-time, with a yes/no outcome.	Identity Dictionary http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html

Other Websites Containing Glossaries of IdM Terms

Other Websites Containing Glossaries of IdM Terms

Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity - Management - A Consolidated Proposal for Terminology
http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Digital Identity - Wikipedia entry
http://en.wikipedia.org/wiki/Digital_identity

ETSI Terms and Definitions Database
http://webapp.etsi.org/Teddi

FIDIS Definitions of Identity
http://www.calt.insead.edu/fidis/definitions

IAMSECT Glossary
http://iamsect.ncl.ac.uk/glossary

Identity Commons2 Identity Schemas - a catalogue of identity-related ontology's (schemas)
http://idschemas.idcommons.net

Identity Gang of Identity Commons
http://www.identitygang.org/moin.cgi/Lexicon

Internet 2 Glossary
http://www.internet2.edu/info/internet2-glossary.cfm

ITU-R/ITU-T Terms and Definitions
http://www.itu.int/pub/R-TER-DB

ITU-T SG17 Compendium of Terms
http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc

Meta-Access Management System (MAMS)
https://mams.melcoe.mq.edu.au/zope/mams/kb/glossary

Modinis-IDM Common Terminological Framework for Interoperable Electronic Identity Management
https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc?code=nldsv13294

NIST IR 7298 - Glossary of Key Information Security Terms
http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

The Open Mobile Alliance Identity Management Framework
http://www.openmobilealliance.org/release_program/rd.html

OpenPrivacy.org definitions page
http://www.openprivacy.org/opd.shtml

SAML 2.0 glossary
http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

Security Guide for Interconnecting Information Technology Systems - NIST SP800-47 Appendix D
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

The Digital Identity Glossary by P.T. Ong with links to other glossaries
http://blog.onghome.com/glossary.htm

The Identity Dictionary Allan Milgate's 100 technical terms for the common understanding of IAM
http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html

Trusted Computing Group Glossary of Technical Terms
https://www.trustedcomputinggroup.org/groups/glossary

W3C Glossary and Dictionary
http://www.w3.org/2003/glossary

Weaving the Web - Berners Lee Glossary
http://www.w3.org/People/Berners-Lee/Weaving/glossary.html

2008–2009 NSTAC Correspondence to the President

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

November 6, 2008

The President
The White House
Washington, DC 20500

Dear Mr. President:

It was a great pleasure to meet with you during the 2008 National Security Telecommunications Advisory Committee (NSTAC) Meeting. The NSTAC would like to commend the Department of Homeland Security's (DHS) continued collaboration and partnership with the NSTAC. We applaud the steps your administration has taken in response to several previous NSTAC recommendations, in particular, those regarding global infrastructure resiliency.

During our discussion, you requested the development of an NSTAC recommendation evaluation process for your administration. The NSTAC values feedback it receives from the Executive Office of the President (EOP) and our Government stakeholders; this feedback allows the NSTAC to better serve our national security and emergency preparedness (NS/EP) goals. While DHS is finalizing a formal feedback process for Government use, we would like to submit for your consideration, four issue areas that we believe should be continuing priorities. We believe continued support and leadership in these areas will enhance our Nation's NS/EP posture and the private sector's ability to support this objective.

- **Government funding of priority programs**—The Government programs for priority telecommunications services and the National Coordinating Center (NCC) are foundational platforms for NS/EP communications. It is important to continue providing adequate funding for development and implementation of the priority telecommunications services such as the Government Emergency Telecommunications Service and the Wireless Priority Service, particularly in light of the network's rapid evolution to Internet Protocols. In addition, the 24/7 NCC for Telecommunications Watch is critical to ensuring NS/EP; funding to sustain and enhance this operation is also important.

- **Information sharing**—Sharing sensitive information between the Government and the private sector is the first, most important step outlined in all Government NS/EP initiatives. We support the continued development of Government process protocols to share information with appropriately cleared public/private personnel who work on NS/EP issues. A key first step is improving the timely sponsorship and issuance of private sector clearances, up to and including a Top Secret/Sensitive Compartmented Information clearance.

- **Credentialing and access**—During your administration, the creation of the essential service provider classification in the *Warning, Alert, and Response Network* (*WARN*) *Act* was a significant step in recognizing the important role of critical infrastructure owners and operators. To significantly enhance the resiliency of our national telecommunications infrastructure, appropriate Presidential guidance is necessary to ensure Government processes define key response personnel of critical infrastructures as essential service providers. Additionally, essential service providers should receive non-monetary Federal assistance under the *Robert R. Stafford Disaster Relief and Emergency Assistance Act* when acting in a mission-assignment capacity.

- **Telecommunications electric power dependency**—The Nation's reliance on power is undisputed. We appreciate the work of the Federal Communications Dependency on Electric Power Working Group, and we look forward to its report on the long-term outage issue, which may have implications in sectors beyond the telecommunications industry.

Over the last year, we have met extensively with your executive office representatives, and their input has been instrumental in shaping NSTAC products. Their continued leadership in the four above-mentioned areas will ultimately result in significant progress toward the goals of strengthening our national security and enhancing the resiliency of our Nation's infrastructure. As the NSTAC moves forward, we welcome continued feedback from the EOP pertaining to the value of our recommendations.

Mr. President, it has been a distinct honor to work with you and your administration these past eight years. On behalf of your NSTAC, we thank you and your administration for your support and your trust in our guidance.

Sincerely,

Edward A. Mueller
NSTAC Chair

Copy to:
The Vice President
Executive Office of the President
Secretary of Homeland Security
Under Secretary for National Protection and Programs, DHS/Manager, National Communications System

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

November 6, 2008

The President
The White House
Washington, DC 20500

Dear Mr. President:

In May 2004, the President's National Security Telecommunications Advisory Committee (NSTAC) began an examination of how the convergence of wireless, wireline, and Internet Protocol (IP) networks into global next generation networks (NGN) would affect national security and emergency preparedness (NS/EP) communications. In March 2005, the NSTAC submitted its *NSTAC Near-Term Recommendations Report on Next Generation Networks* to the President, recommending short-term actions that Federal departments and agencies could take to immediately preserve or enhance NS/EP communications for the future. The NSTAC then submitted a follow-on *NSTAC Report on Next Generation Networks* to the President in March 2006. The 2006 *Report* offered recommendations regarding the Government's ability to support NS/EP functional requirements over the NGN and also provide greater capabilities to NS/EP users.

During the 2008 NSTAC Annual Meeting, the NSTAC Principals agreed to re-examine the previous NGN work with two purposes:

- To closely examine the 2006 *Report* recommendations and to identify and review current Federal Government efforts that address issues in the report's recommendations; and

- To identify gaps among the 2006 *Report* recommendations, current NGN needs related to the provisioning of NS/EP communications, and existing Federal Government activities, and to provide follow-up recommendations to ongoing work and to enhance future Federal NGN NS/EP activities and implementation actions.

The NSTAC recognizes that numerous departments and agencies are actively addressing NGN transition issues. Many of the NSTAC recommendations from its 2005 and 2006 NGN reports have been acted upon, and the NSTAC commends these important efforts. To further contribute to the momentum of the Government's activities in the NGN area, the NSTAC seeks to share with appropriate departments and agencies additional follow-up implementation suggestions, as detailed in the attachment to this letter, that support NGN NS/EP capabilities.

These suggested enhancements to current Government efforts address the original 2006 *NGN Report* recommendation areas of:

- Identity management
- Coordination on common operational criteria for NGN NS/EP end-to-end services
- Research and development

- Technology lifecycle assurance and trusted technology
- Resilient alternate communications
- Agreements, standards, policy, and regulations
- Incident management on the NGN
- International policy
- First responders.

In addition, the NSTAC encourages the Federal Government to continue to provide the resources necessary to aid the development, implementation, and maintenance of these NGN NS/EP activities. With your support, the NSTAC stands ready to work with the Executive Office of the President to further examine and address these suggested implementation areas, as needed. We appreciate the continued involvement of executive branch representatives regarding NSTAC recommendations and hope that these recommendations enhance related Federal Government initiatives.

We look forward to working with you, Mr. President, and with your administration on critical telecommunications issues. The NSTAC thanks you for your consideration of these recommendations.

Sincerely,

Edward A. Mueller
NSTAC Chair

Attachment:
Summary of 2006 *NSTAC Report on Next Generation Networks* Recommendations with Suggestions for Implementation Enhancements

Copy to:
The Vice President
Secretary of State
Secretary of Defense
Secretary of Homeland Security
Secretary of Commerce
Director, Office of Management and Budget
Assistant to the President for National Security Affairs
Assistant to the President for Homeland Security
Assistant to the President for Science and Technology
Under Secretary for National Protection and Programs, DHS/Manager, National Communications System
Assistant Secretary for Cybersecurity and Communications, DHS
Director, National Communications System
NSTAC Principals and Industry Executive Subcommittee Members

ATTACHMENT

Summary of 2006 *NSTAC Report on Next Generation Networks* Recommendations with Suggestions for Implementation Enhancements

Identity Management (NGNTF 2006-1)
The NSTAC originally recommended that multiple Federal Government organizations partner with the private sector to build a federated, interoperable, survivable, and effective identity management (IdM) framework for the NGN. We repeat that recommendation, as updated to include whatever Federal organizations assume or may be assigned leadership in Federal interagency IdM plans and processes. The NSTAC suggests the following enhancements to current agency activities:

- Review the recommendations in the Office of Science and Technology Policy (OSTP) National Science and Technology Council's Subcommittee on Biometrics and Identity Management *Identity Management Task Force Report* released in September 2008, with particular emphasis on the requirements associated with industry and Government partnership around technology standards, governance, and research and development (R&D) investments;
- Review the recommendations that resulted from the IdM session of the September 2008 NSTAC R&D Exchange that called for improved IdM coordination, with a focus on national security and emergency preparedness (NS/EP) communications in future R&D activities; and
- Leverage ongoing Department of Defense (DOD) work to determine if it may be applied to broader agency efforts for an NS/EP NGN communications framework and architecture.

Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services (NGNTF 2006-2)
Building on the recommendation to direct the OSTP, with support from National Communications System (NCS) agencies, to establish a joint industry-Government initiative to create a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN, that would include a regular NGN summit to coordinate planning, measure progress of efforts, and recommend and monitor programs that would foster NS/EP capabilities within the NGN, the NSTAC suggests the following enhancements to current agency activities:

- Continue to coordinate across departments and agencies and with the private sector to establish a Common Operational Criteria development framework, and more closely organize NGN standardization and R&D requirements;
- Create a regular NGN summit with the communications and information technology sectors, Government, and other private sector stakeholders to discuss an end-to-end solution; and
- Review the *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic* of November 2008 that examines risks associated with Internet Protocol-based (IP) NS/EP communications and priority service traffic and presents recommendations to ensure the service delivery. These include managing traffic through quality of service programming in routers, and expanding the use of managed service agreements to provision NS/EP services within the new IP-based environment.

Research and Development (R&D) (NGNTF 2006-3)
Building on the recommendation to direct OSTP, with support from other relevant agencies, especially DHS, National Institute of Standards and Technology (NIST), and DOD, to establish and prioritize initiatives that will foster collaborative and coordinated R&D supporting a Common Operational Criteria

and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/information technology and service providers, the NSTAC suggests the following enhancements to current agency activities:

- Develop a more coordinated mechanism by which participants in R&D initiatives can collaborate and test R&D technology and capabilities on the NGN, including joint-testing, information sharing on emerging NGN technologies, and analysis of existing technologies;
- Ensure that departments and agencies collaborate more closely with the private sector to improve the technology transfer between Government-funded research and industry development;
- Ensure appropriate programs focus on long-term and short-term NGN R&D as it relates to supporting critical NS/EP communications capabilities to help prioritize initiatives for optimal resource allocation; and
- Ensure collaboration with private industry to include NGN NS/EP communications user requirements in the R&D efforts associated with the Comprehensive National Cybersecurity Initiative (CNCI), and the Networking and Information Technology Research and Development Program's Cyber Security and Information Assurance Program and the High Confidence Software and Systems R&D program, as appropriate.

Technology Lifecycle Assurance and Trusted Technology (NGNTF 2006-4)
Building on the recommendation to direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of technology lifecycle assurance mechanisms and innovative trusted technologies that reduce the presence of intrinsic vulnerabilities, the NSTAC suggests the following enhancements to current agency activities:

- Examine and consider incorporating industry models and best common practices into the complete NGN technology lifecycle as it applies to NS/EP communications, to include NGN hardware and software acquisition processes; supply chain assurance; and technology development;
- Coordinate with the private industry to better understand global sourcing models, including how these models incorporate risk management and how to address risk resulting from globalized supply chains; and
- Ensure coordination with and input from industry in the preparation for and implementation of any forthcoming supply chain risk management guidance resulting from the CNCI.

Resilient Alternate Communications (NGNTF 2006-5)
Building on the recommendation to direct OMB and DHS to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment through emergency plans, analyses of alternative NGN access methods against threat scenarios, and augmentation and replacement methods for damaged or diminished access to the communications infrastructure, the NSTAC suggests the following enhancements to current agency activities:

- Recognizing that NCS Directive 3-10, *Minimum Requirements for Communications Continuity*, addresses most suggestions in this recommendation, continue investigating technology solutions that will address IP priority solutions, NGN threat opportunities, and/or network resiliency assurance; and
- Review the recommendations in the *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic* of November 2008 that examines resilient, alternative communications.

Agreements, Standards, Policy, and Regulations (NGNTF 2006-6)
Building on the recommendation to direct DHS, the Department of State, and DOC (including NIST and the National Telecommunications and Information Administration) to engage and coordinate among domestic and international entities to ensure that policy frameworks established through Agreements, Standards, Policies, and Regulations support NGN NS/EP capabilities in a globally distributed NGN environment, the NSTAC suggests the following enhancements to current agency activities:

- Improve coordination among DHS, DOS, DOC, and other agencies as appropriate, when engaging with domestic and international policy and standards entities in order to develop a more consistent, unified U.S. strategy;
- Ensure that policy frameworks support NGN NS/EP capabilities in the U.S. and on the international level, including end-to-end NS/EP capabilities on separate NGN and legacy networks as well as when these networks converge; and
- Review the *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic* of November 2008 for additional recommendations to ensure networks remain capable of providing priority communications for NS/EP authorized users.

Incident Management on the NGN (NGNTF 2006-7)
Building on the recommendation to direct DHS to establish an NGN incident response capability that includes a Joint Coordination Center for all key sectors, and with supporting mechanisms such as a training academy, exercise program, and R&D program, the NSTAC suggests the following enhancements to current agency activities:

- Increase intergovernmental coordination to address incident management, including the development of standard operating procedures and greater interaction between cyber centers, private industry, and international entities, especially on cyber security issues;
- Further promote private industry and Government collaboration by establishing a protocol for routine engagement between the U.S. Computer Emergency Readiness Team and information technology and communications industry representatives; add explicit linkages for industry interaction during times of crisis to the standard operating procedures of the National Cyber Response Coordination Group; and involve industry participation in the establishment of the National Cyber Security Center; and
- Investigate the existence of additional technologies, tools, and capabilities available to help strengthen DHS NGN incident response.

International Policy (NGNTF 2006-8)
Building on the recommendation to direct departments and agencies to develop cohesive domestic and international NS/EP communications policy, including intergovernmental cooperation mechanisms to harmonize NS/EP policy regimes, rules of engagement for non-U.S. companies in NS/EP incident response in the United States, and information sharing and response mechanisms in the international NGN environment, the NSTAC suggests the following enhancements to current agency activities:

- Improve interagency coordination of NS/EP communications policy requirements and activities across the Federal government. In particular, continue to develop the intergovernmental cooperation mechanisms and rules of engagement for non-U.S. companies in incident response, specifically when engaging with international entities or standards bodies; and ensure that international standards and policies support global, end-to-end NS/EP communications.

First Responders (NGNTF 2006-9)
Building on the recommendation to direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, the NSTAC suggests the following enhancements to current agency activities:

- Emphasize the importance of the implementation of NGN systems, protocols, and processes at the first responder level while systems undergo the lengthy transition from legacy networks and services.

Office of the Manager
National Communications System
Customer Service Division

Mail Stop 8510
245 Murray Lane
Washington, DC 20528-8510
(703) 235-5525

www.ncs.gov/nstac/nstac.html
nstac1@dhs.gov