2008 Research and Development Exchange Workshop Proceedings

Evolving National Security and Emergency Preparedness (NS/EP) Communications in a Global Environment

Sponsored by the Industry Executive Subcommittee's Research and Development Task Force of the President's National Security Telecommunications Advisory Committee

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.

RESEARCH AND DEVELOPMENT EXCHANGE WORKSHOP PROCEEDINGS

1.0 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.

187

[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.

- **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.

2.0 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 user-centric 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 high-speed 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 self-actualization 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 re-configurability. 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, self-managing 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 cross-sector 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 cross-domain attack correlation technologies, real-time 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 high-performance 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 leap-ahead 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.

3.0 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.

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

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?

- 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.

Figure 1. Emergency Communications Response Networks Agenda for Action

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

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 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.

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

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

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 following table (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.

Figure 3. Convergent Technologies Agenda for Action

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

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 industry-Government collaboration on cyber defense; when executed effectively, these public-private 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. 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.

Figure 4. Defending Cyberspace Agenda for Action

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

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 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 following table (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.

Figure 5. Identity Management Agenda for Action

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

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:

- **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 on-demand 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 following table (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.

Figure 6. Emerging Technologies Agenda for Action

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

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.

Figure 7. Summary of Breakout Session Themes Matrix

	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

4.0 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.

APPENDIX A

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

APPENDIX B

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
CSC

Michael Daly
Raytheon Company

Robert Dix, Jr.
Juniper Networks, Incorporated

Dave Dobbs
Northrop Grumman Corporation

Kathy Downie
Advanced Research & Technology Center

John Edwards
Nortel Networks Corporation

Douglas Egan
CSC

David Ehinger
Rolls-Royce North America

Al Evans
CSC

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
CSC

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
CSC

APPENDIX C

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**

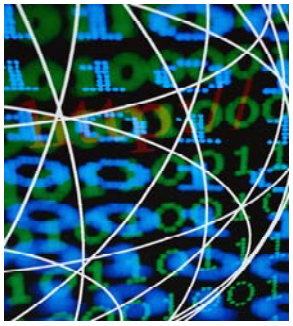
Government & Public Safety

Significant Technology Shifts

1

Technology shift

WWW

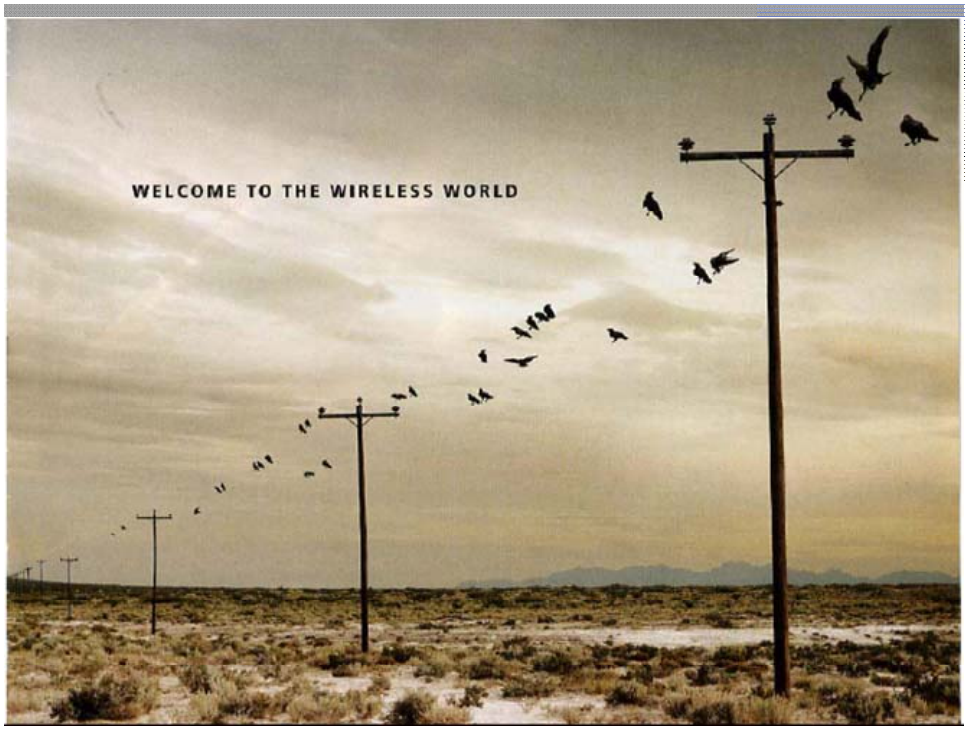


Government & Public Safety

Implications

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

Digital content and information now becomes more valuable.



Significant Technology Shifts

3

Technology shift

Cloud computing

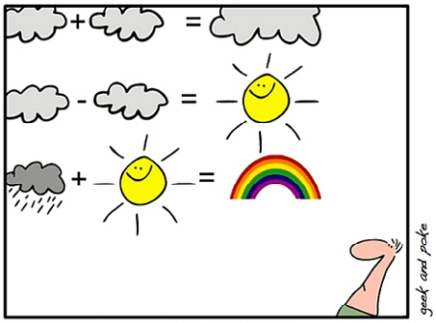
GARTNER Aug 2008: "Organisations are switching from company-owned hardware and software assets to per-use service-based models. This will impact the industry in various ways," Mr. Tully said. "The projected shift to cloud computing, for example, will result in dramatic growth in IT products in some areas 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

Government & Public Safety

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

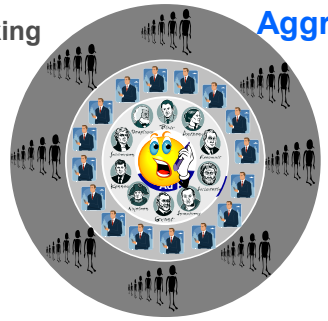
Significant Technology Shifts

5

Technology shift

Web based hosted applications

- Digital content
- Social networking



Government & Public Safety

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

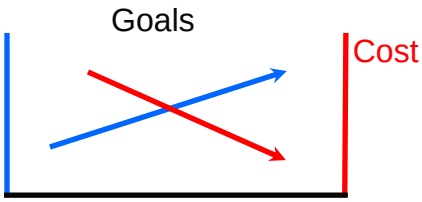
YouTube Broadcast Yourself™

myspace.com a place for friends

facebook

the challenge

Value
- Function
- utility



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

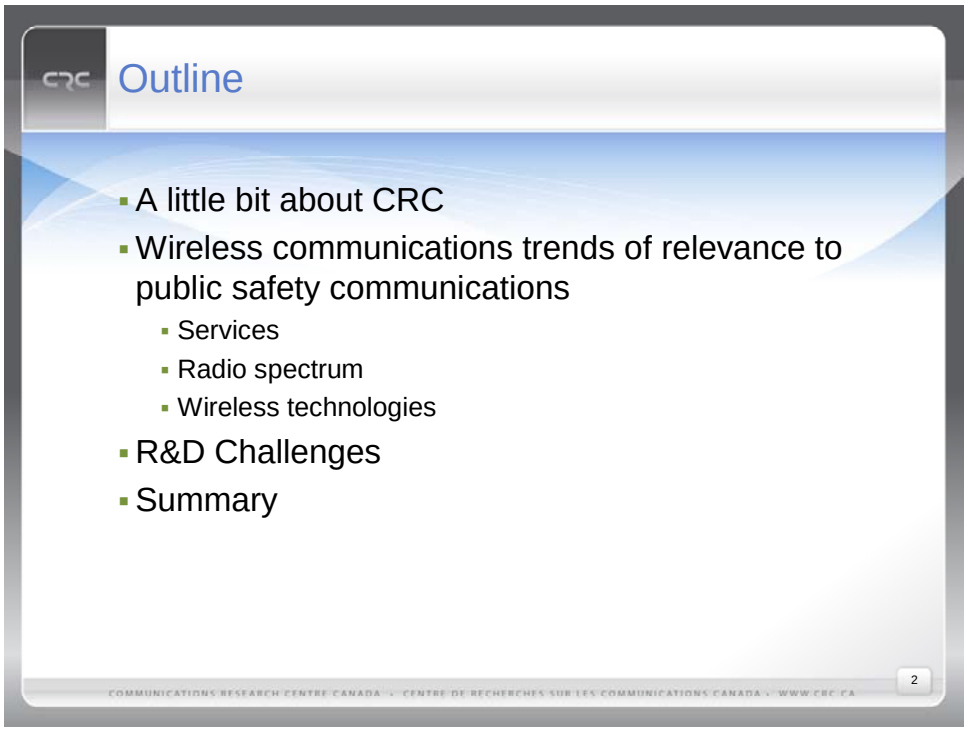
A challenge to us all:

"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

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

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)

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

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

5

Wireless Communications Trends ……

Potential to impact/alter public safety communications

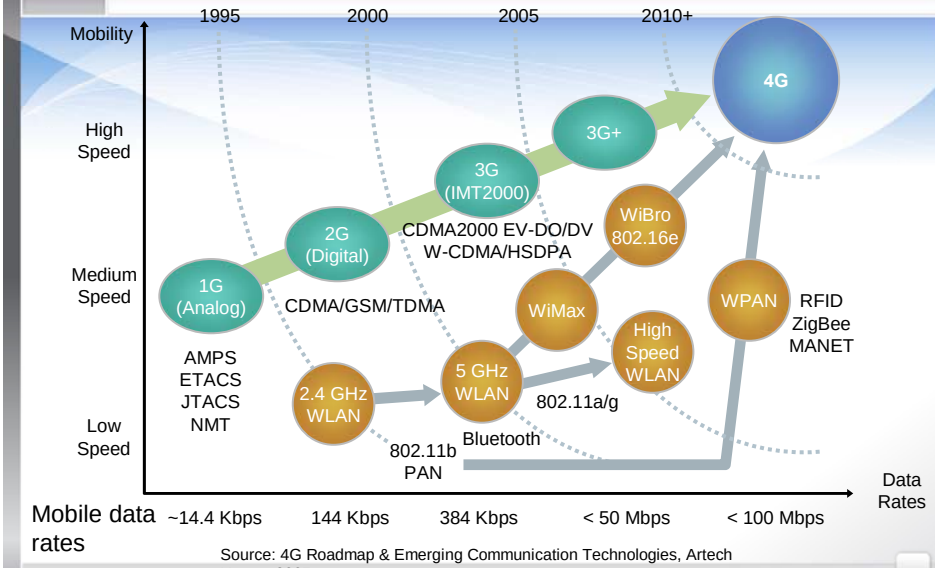
6

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

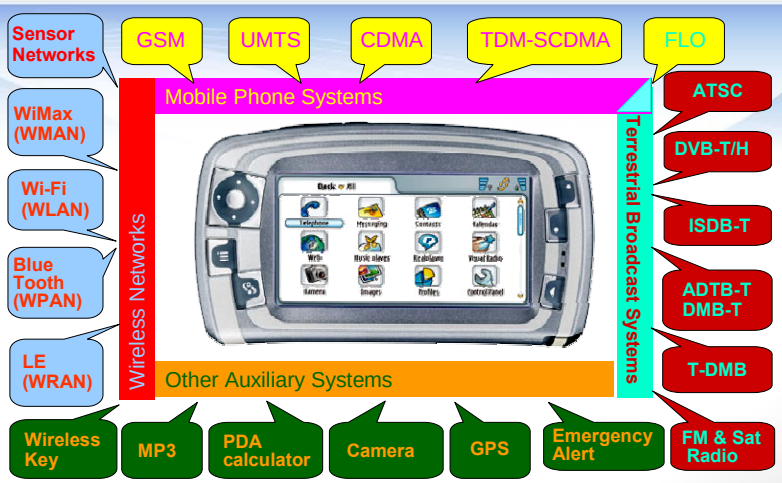
Broadcasting Service Trends

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

Service Convergence on Mobile Handset



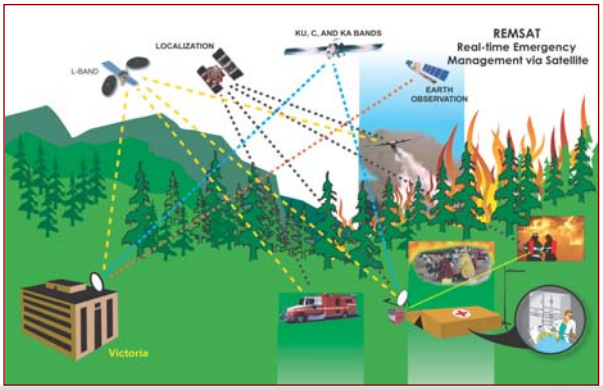
Universal Multimedia Handset

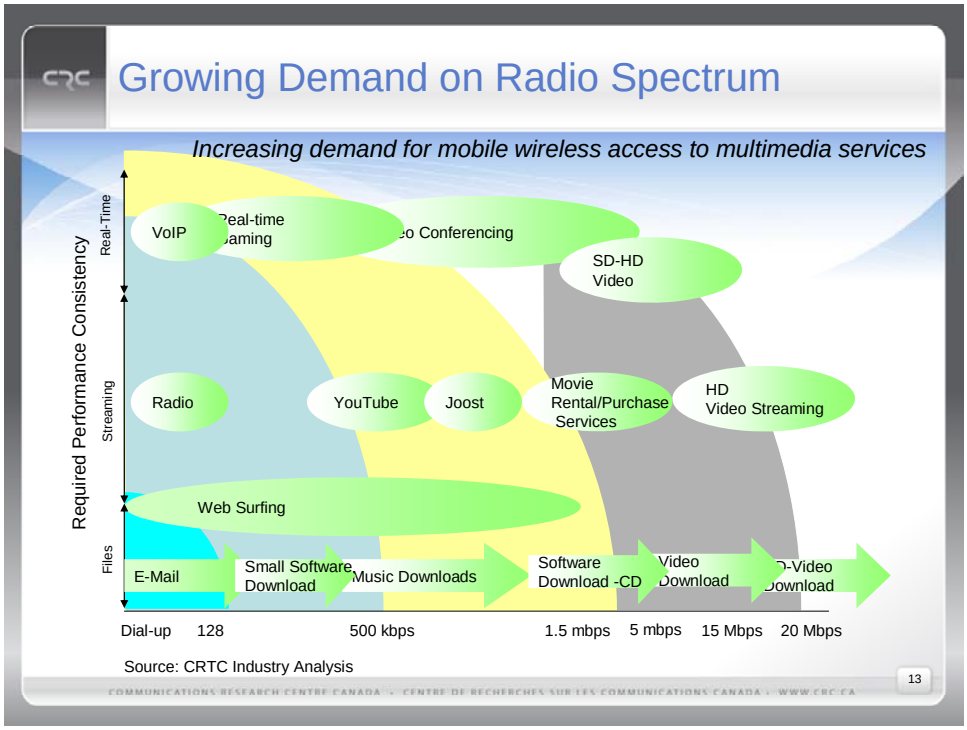
Emergency Alerting Over Wireless Networks

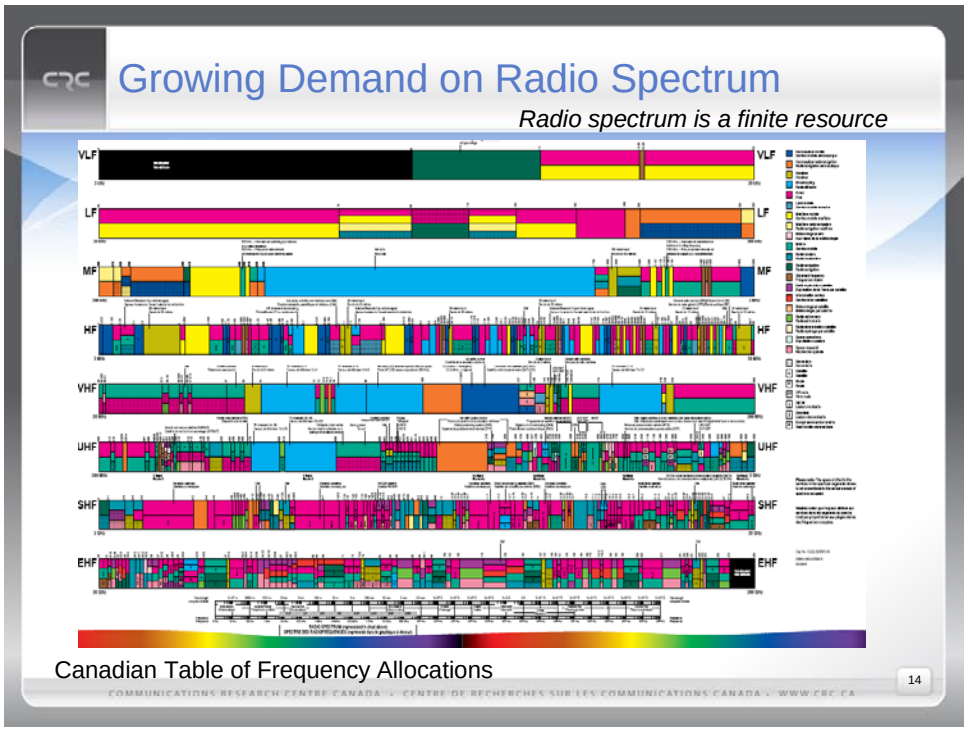
- *Traditional* - Radio and TV broadcasting
- *Emerging* - Alerting to handheld wireless devices
  - Cellular – SMS
    - Challenges include – timely delivery of message to all; network congestion; network failure
  - New multimedia digital broadcasting systems
    - Broadcast networks are efficient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

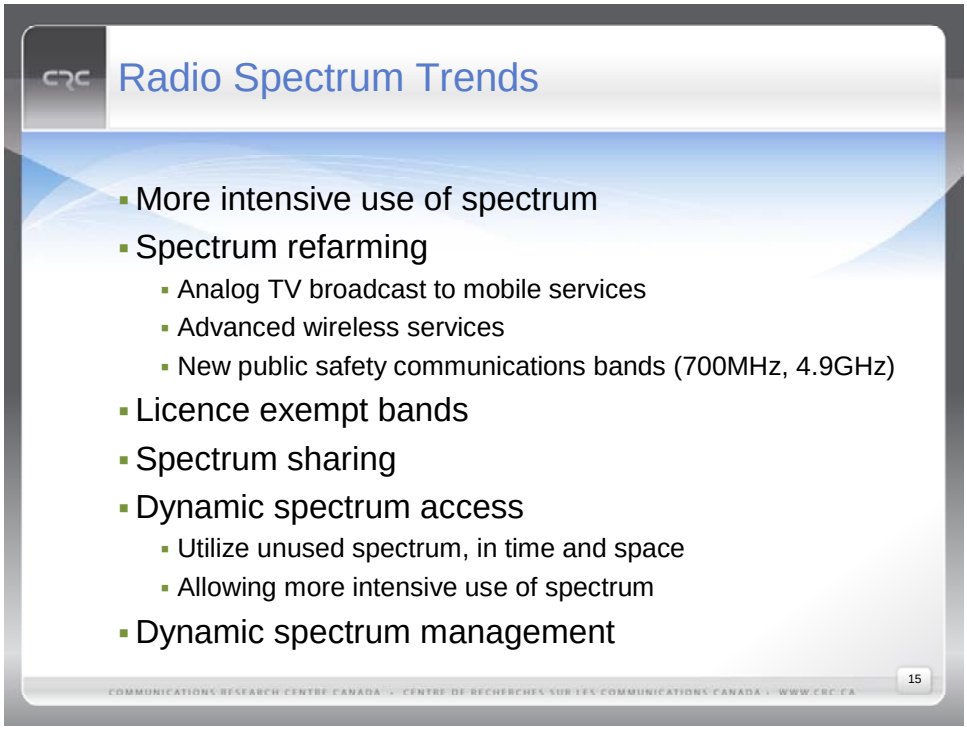
Other Satellite Communications Applications

- 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
eo 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
D-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

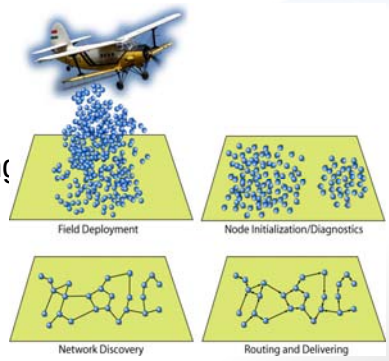

Wireless Technology Trends ……
Potential to impact/alter public safety communications
16

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

Wireless Sensor Networks

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

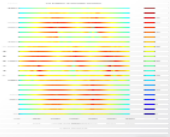


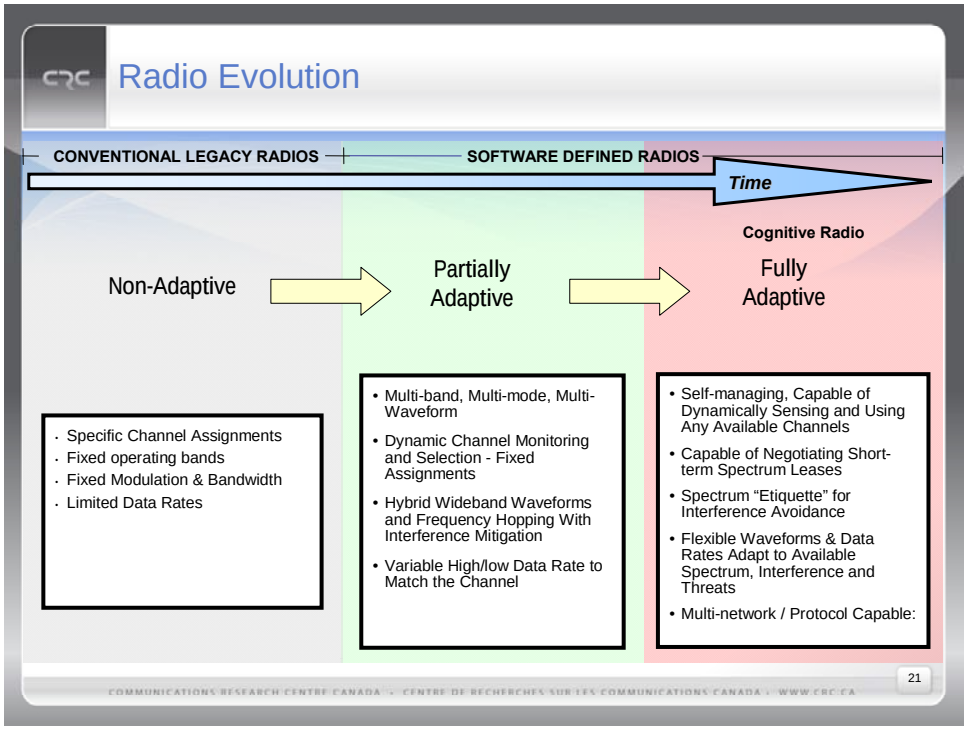
Software Defined Radio - SDR

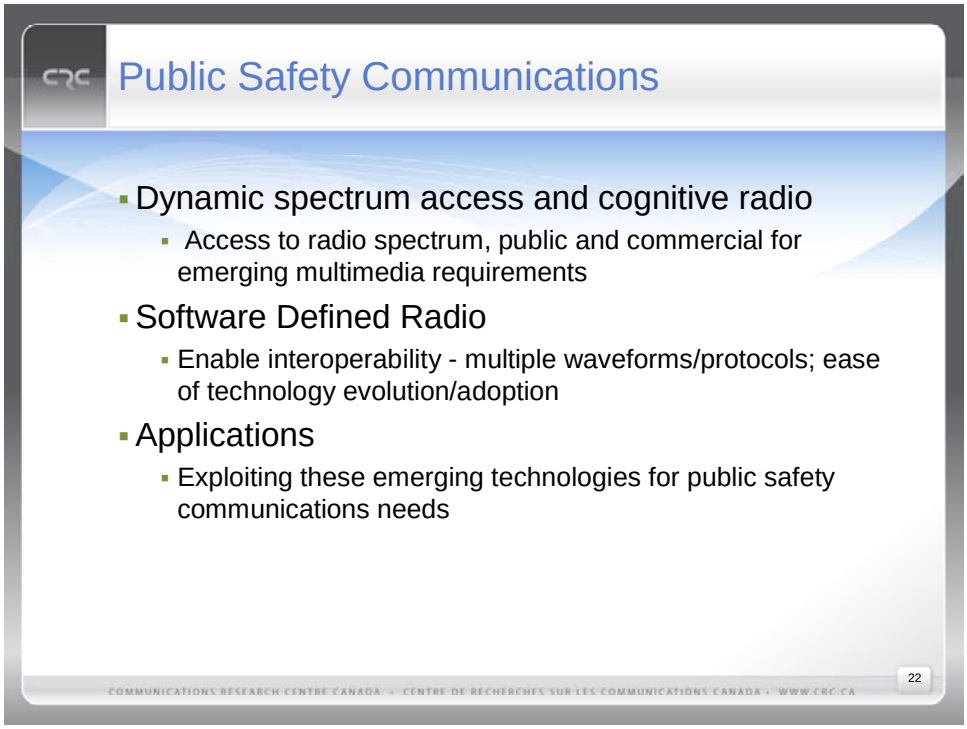
- Radio in which some or all of the physical layer functions are software defined
- SDRs could simultaneously support multiple protocols across a range of spectrum
- SDR Benefits
  - Interoperability
  - Reconfigurability

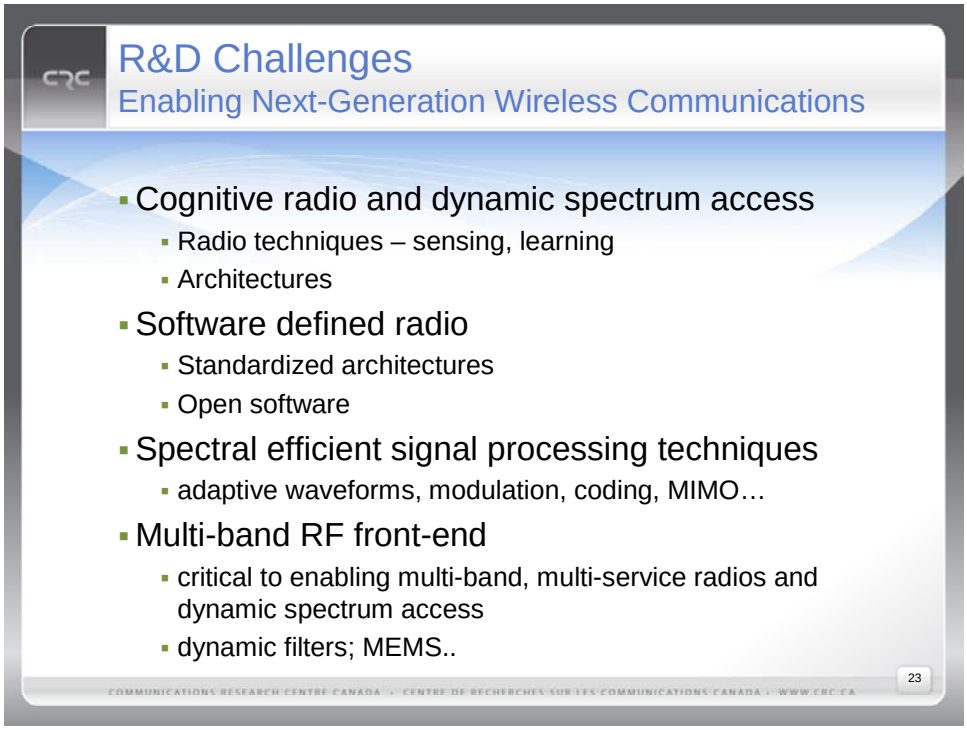
Cognitive Radio

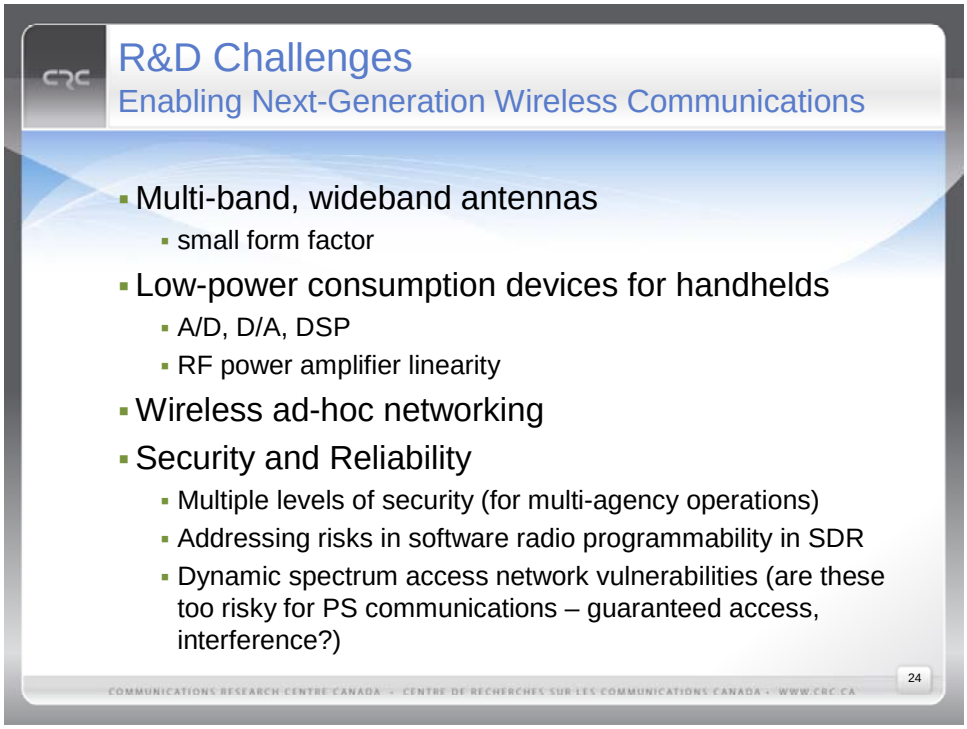
- A radio that senses and is aware of its operational environment and can dynamically and autonomously adjust its radio operating parameters accordingly
- Enables spectrum agile radios and dynamic spectrum access
- Enables improved spectral efficiency, through adaptive optimized use of waveforms, modulation,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

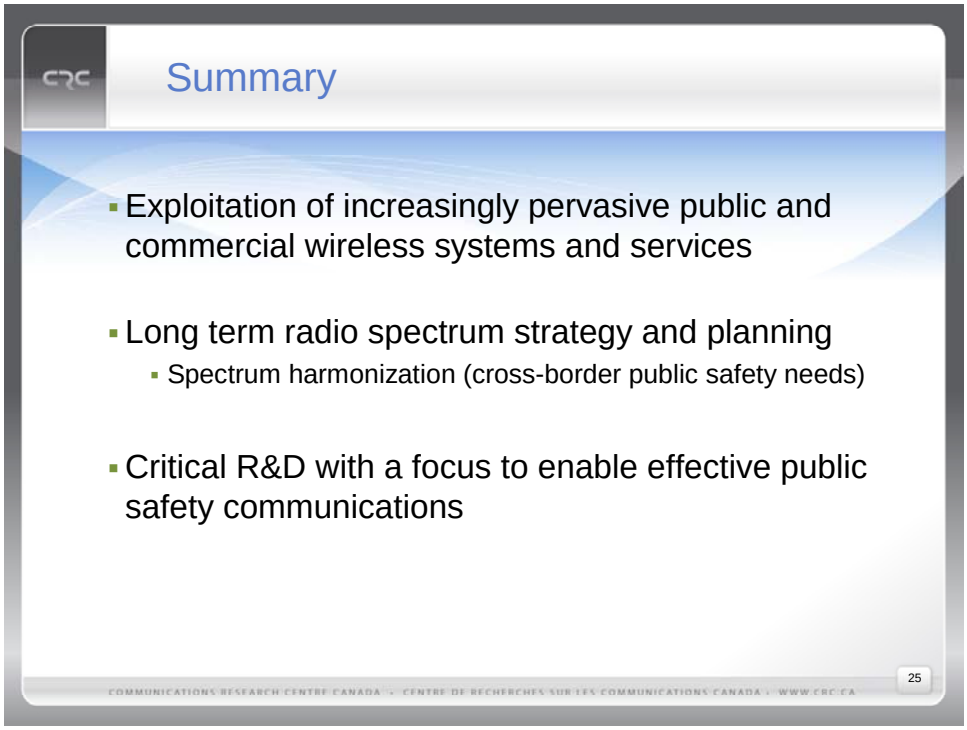



Radio Evolution
CONVENTIONAL LEGACY RADIOS
SOFTWARE DEFINED RADIOS
Time
Cognitive Radio
Non-Adaptive
Partially Adaptive
Fully Adaptive
· Specific Channel Assignments
· Fixed operating bands
· Fixed Modulation & Bandwidth
· Limited Data Rates
• Multi-band, Multi-mode, Multi-Waveform
• Dynamic Channel 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


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


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

Presentation – Ms. Leslie Sibick

Infrastructure Analysis and Strategy Division (IASD) Research and Development Analysis Branch

Infrastructure Protection R&D Process and Priorities

Presented September 2008 by Leslie Anne Sibick, Branch Chief, Research and Development Analysis

Homeland Security

IP R&D Collaboration & Coordination

- **DHS S&T Programs**
  - – Integrated Product Team (IPT) Transition Program
  - – S&T Research and Innovation programs
  - – Centers of Excellence (numerous universities & research institutes with specialized R&D capabilities)
  - – National Institute for Hometown Security
    - •Kentucky Critical Infrastructure Protection (KyCIP)
  - – Southeast Regional Resiliency Initiative (SERRI)

CIKR Sectors

– **Cross Sector R&D Working Group**, co-chaired by IP and S&T, provides forum to discuss common areas of concern, collaborate on cross-sector R&D projects, and develop sector R&D relationships

– **Tiger Teams** assisted in articulating R&D gaps; R&D guidance provided template to elicit desired specificity

Homeland Security FOR OFFICIAL USE ONLY 2

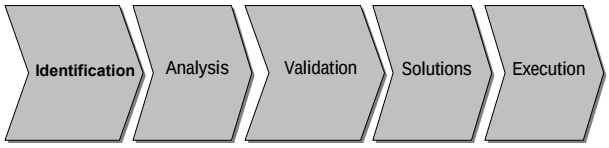
NIPP R&D Requirements Process

- 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)

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



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

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


DEPARTMENT OF
U.S.
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

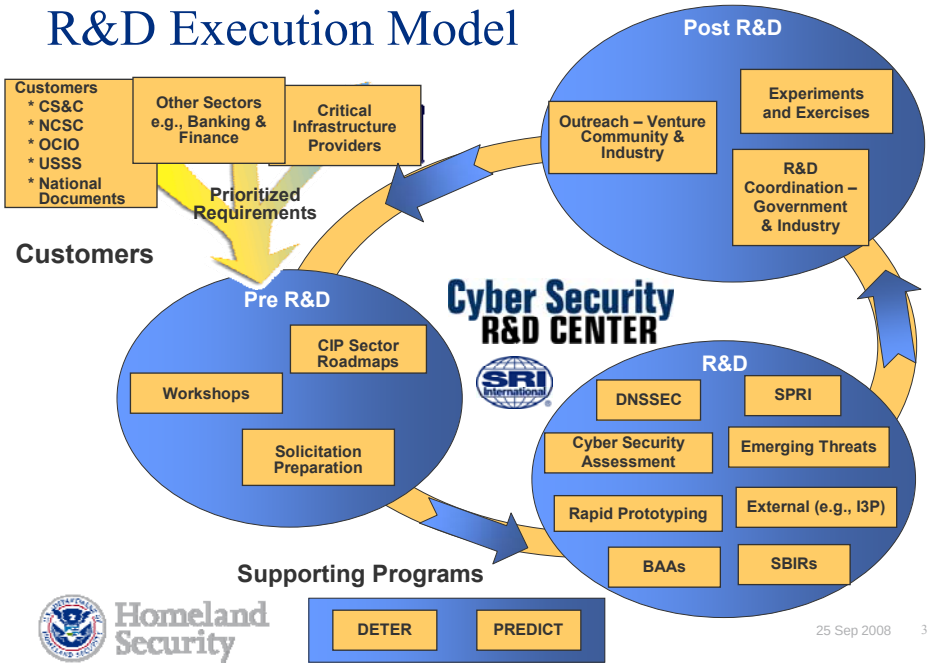
Homeland Security

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 information*
  - 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

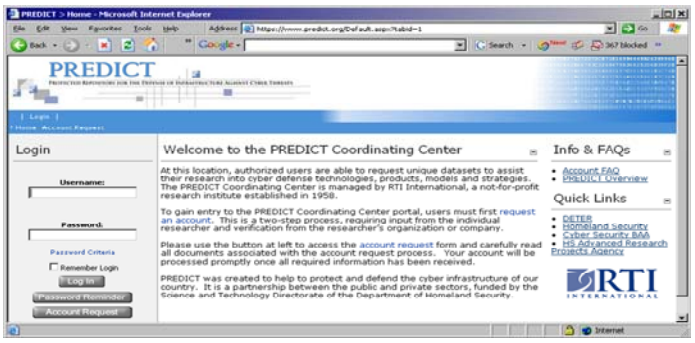
- Classes of data that are interesting, people want collected, and seem reasonable to collect
  - Netflow
  - Packet traces – headers and full packet (context dependent)
  - Critical infrastructure – BGP and DNS data
  - Topology data
  - IDS / firewall logs
  - Performance data
  - Network management 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

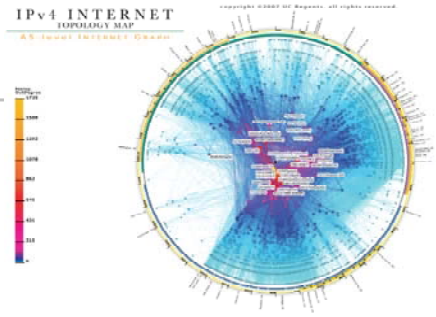
TTA	Type	PI Organization	Paper Title	Time	Proposed Funding
1	II	Georgia Institute of Technology	Countering Botnets: Anomaly-Based Detection, Comprehensive Analysis, and Efficient Mitigation	24	$ 1,050,730
2	I	IBM Thomas J. Watson Research Center	Montage: A Methodology for Designing Composable End-To-End 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

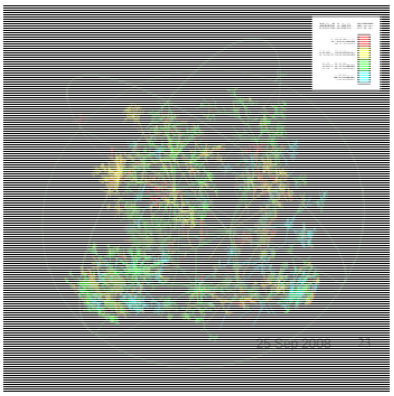
- 5 Academic (CA,GA,WA,CO,MD)
- 8 Private Sector (NY,CO,CA,FL)
- 1 National Lab (NM)

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

25 Sep 2008 25

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**

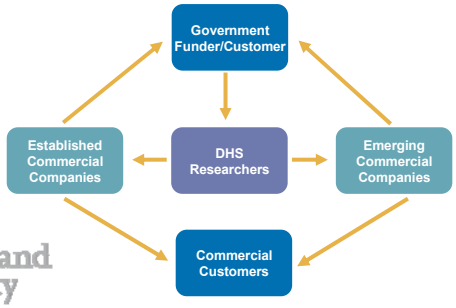
- Botnet Command & Control Detection and Mitigation
  - Examine defenses needed to counter new methods of Botnet C&C

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

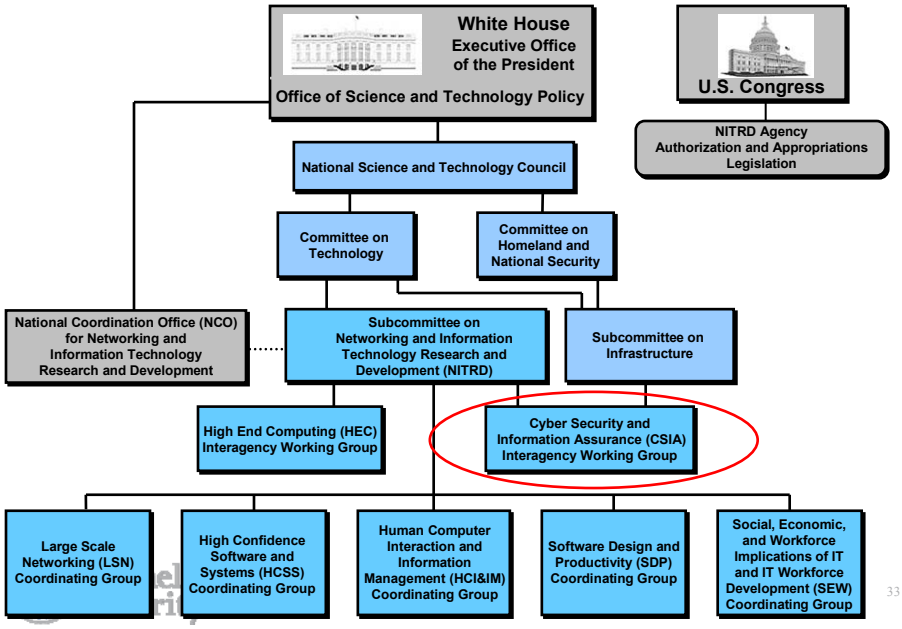
IT Security Entrepreneur Forum (ITSEF)

- 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

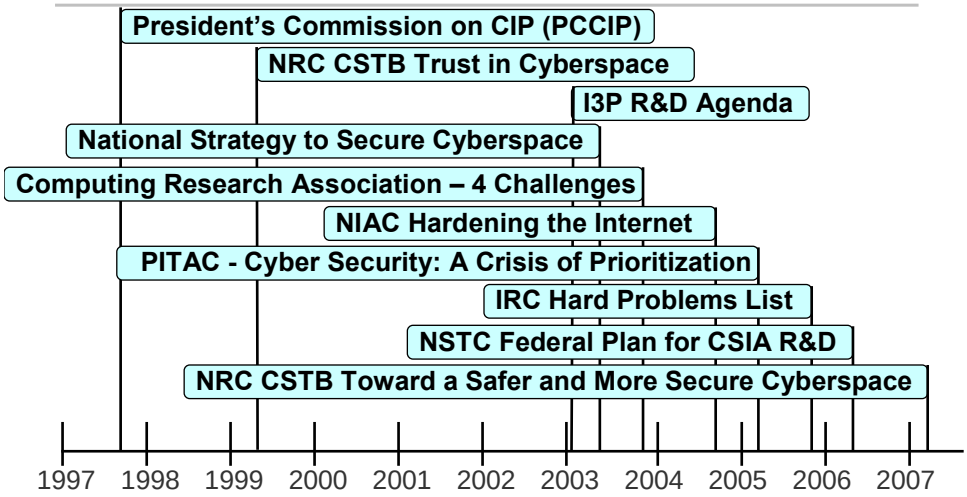
25 Sep 2008 32

NITRD Program Coordination



33

Timeline of Past Research Reports



All documents available at http://www.cyber.st.dhs.gov

Homeland Security

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

For more information, visit
http://www.cyber.st.dhs.gov

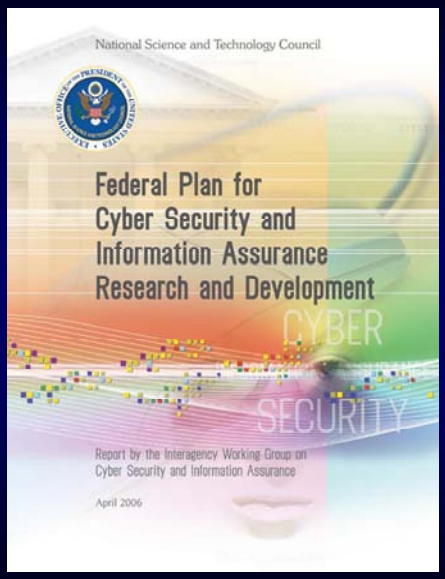
Presentation – Dr. Chris Greer

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

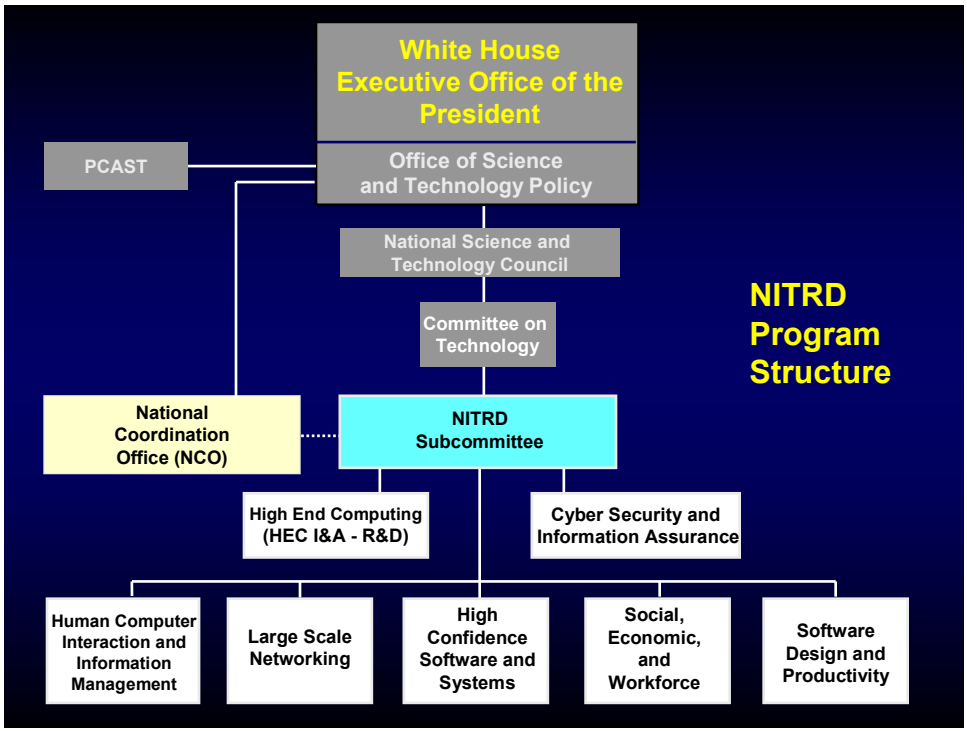
- Improved security for computing and networking systems in Federal and other realms.
- Long-term basic and applied research on high-performance computing, networking systems, and related software.
- Access by the U.S. research community to high-performance computing and networking systems.
- NIT capabilities 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

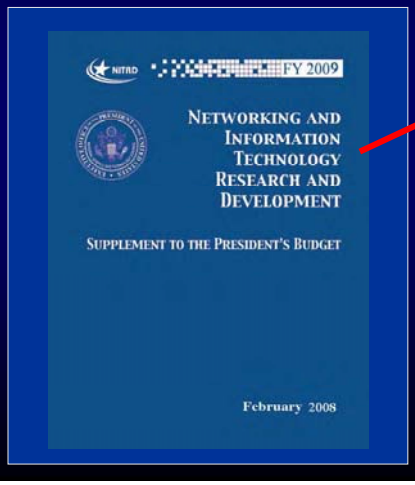
NOAA National Oceanic and Atmospheric Administration

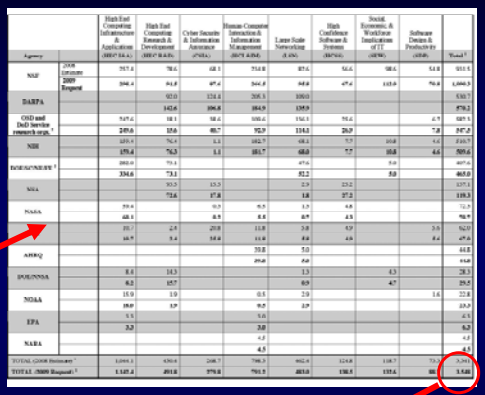
NSA National Security Agency

NSF National Science Foundation

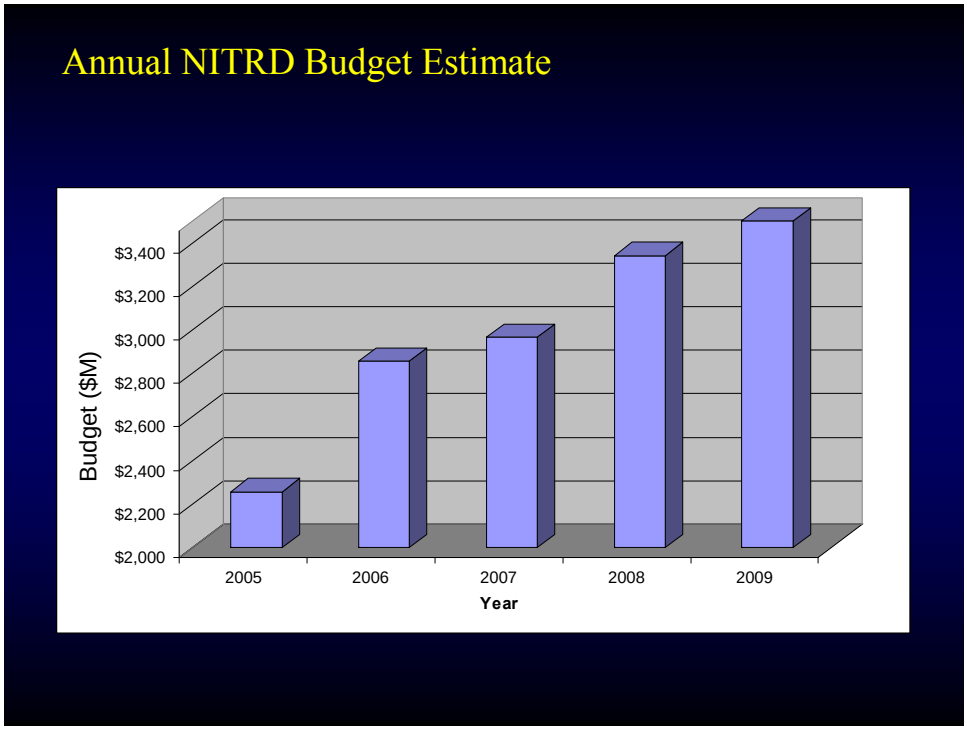
OSD and DoD Service research organizations, Office of the Deputy, Under Secretary of Defense (Science and Technology)

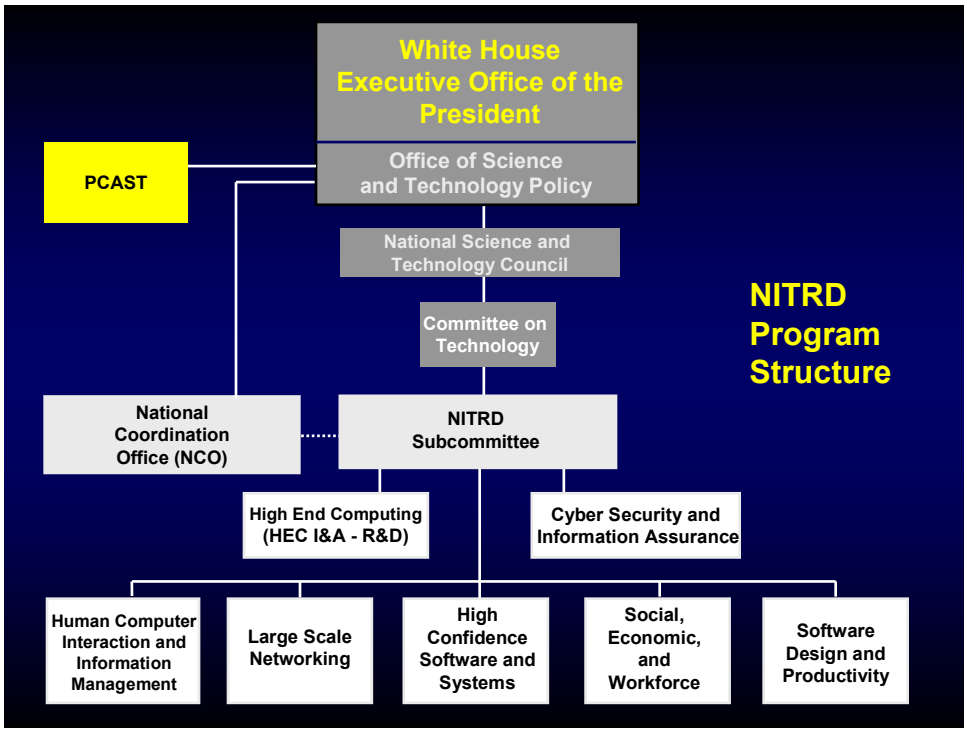
FY 2009 Supplement to the President's Budget for the NITRD Program





$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

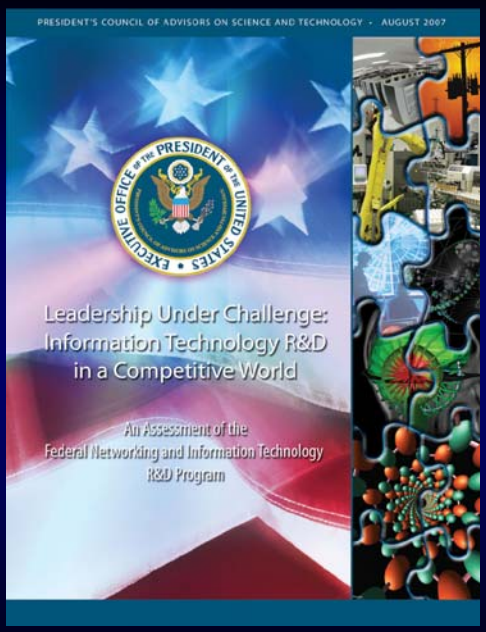
Under Executive order 13226, PCAST ..

… 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

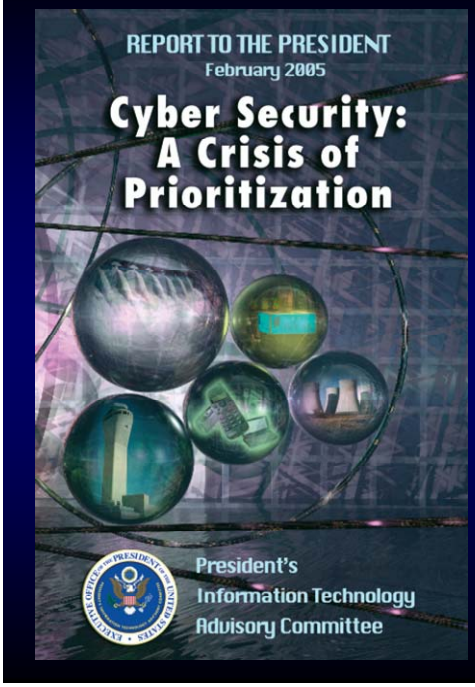
- Findings
  - In general, the NITRD Program has effectively balanced statutory mandates and agency mission requirements
  - However, the NITRD Program's *current coordination processes are inadequate* to meet anticipated national needs and to maintain U.S. leadership in a globally competitive world
- 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

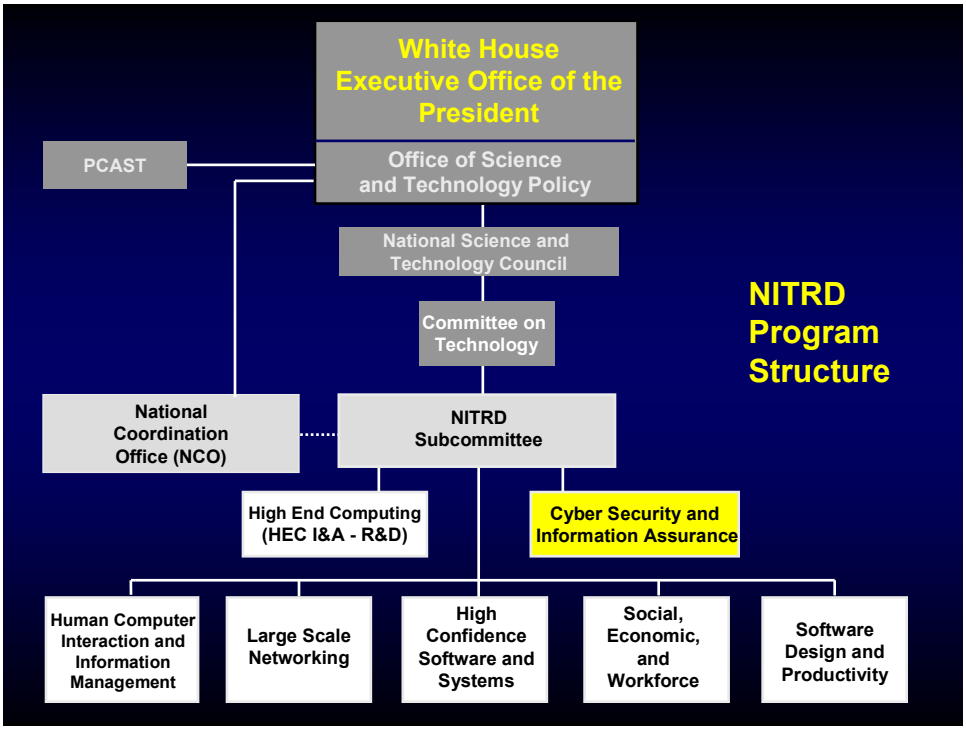
RFI — Open Workshop — Public Comments

Strategic Framework — **Draft Text** — **Final Text**

www.nitrd.gov



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.



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

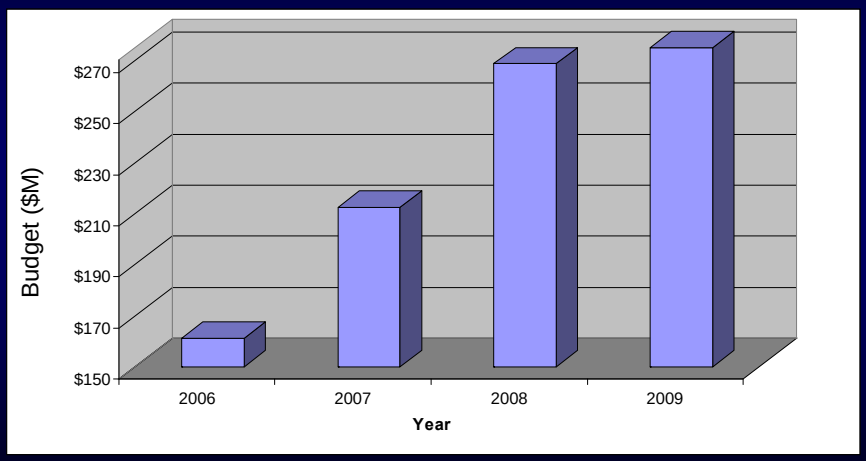
NIST National Institute of Standards and Technology

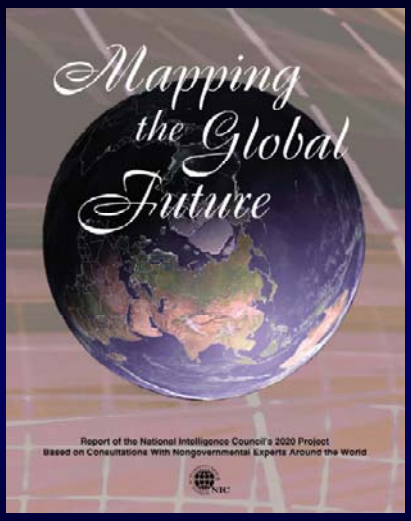
NSA National Security Agency

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.*"

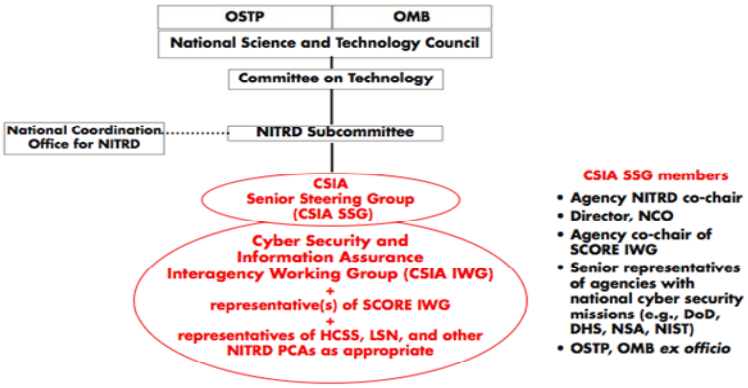
Principles for Multidimensional Cyber R&D:

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



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

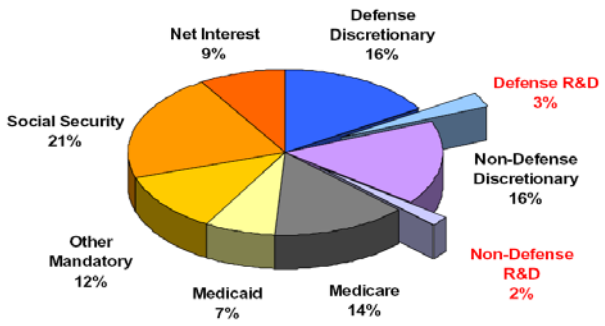
Plenary Address – Ambassador Richard Russell

NSTAC R&D Exchange

Ambassador Richard M. Russell

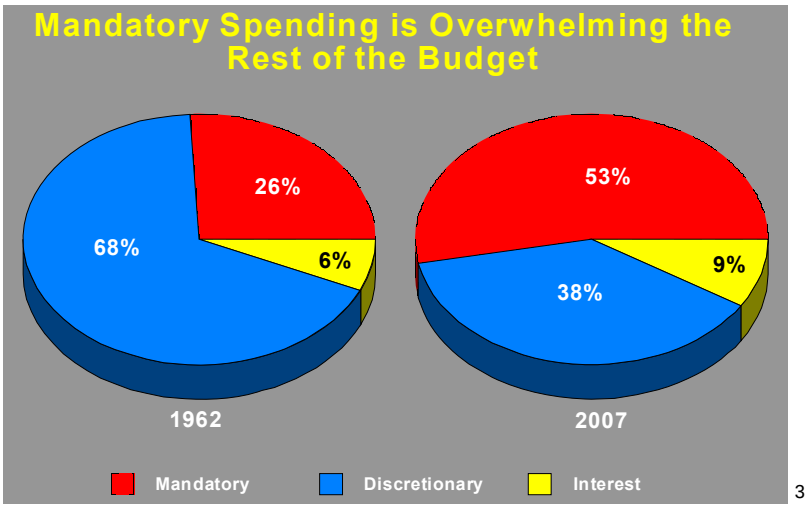
Associate Director and Deputy Director for Technology
Office of Science and Technology Policy
Executive Office of the President

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



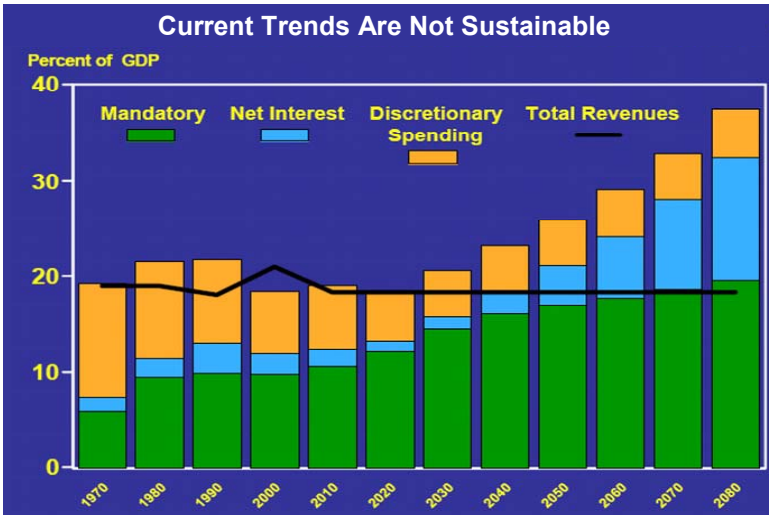
R&D = 15% of discretionary spending

Mandatory Spending Growth (1962-2007)



3

Long-term Fiscal Outlook

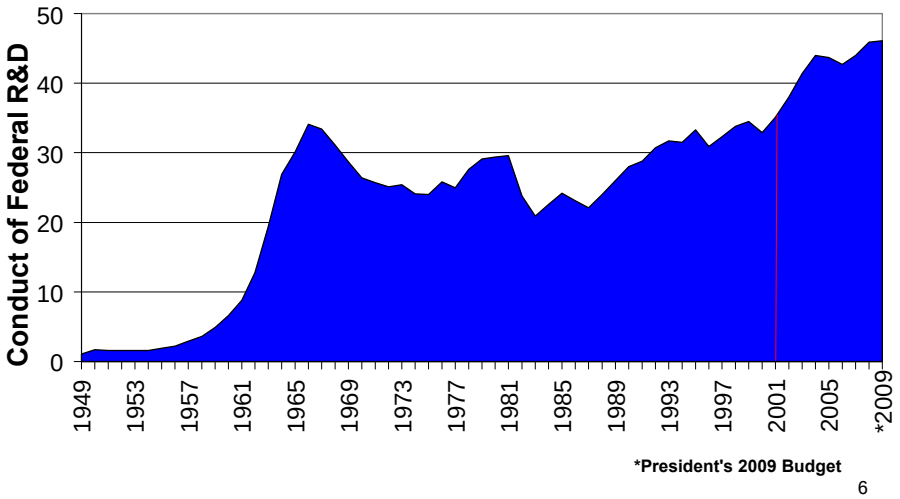


FY2009 R&D Highlights

- 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.

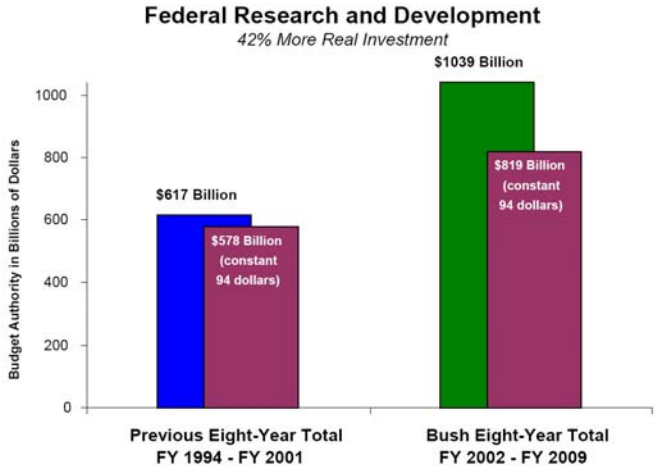
5

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



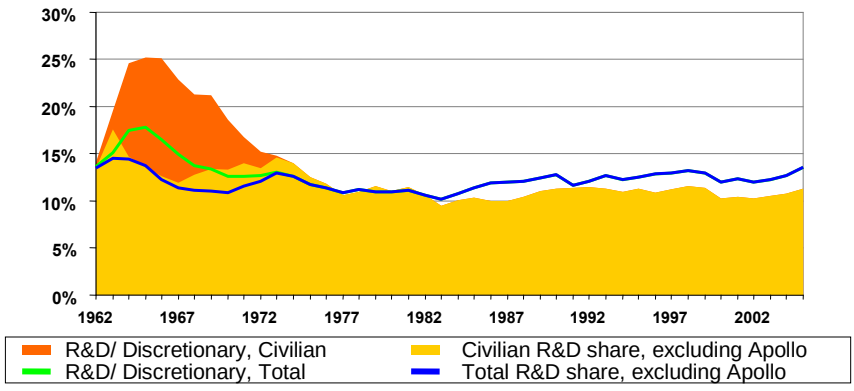
6

R&D Spending Comparisons: Administration to Administration



R&D as a Share of Discretionary Spending

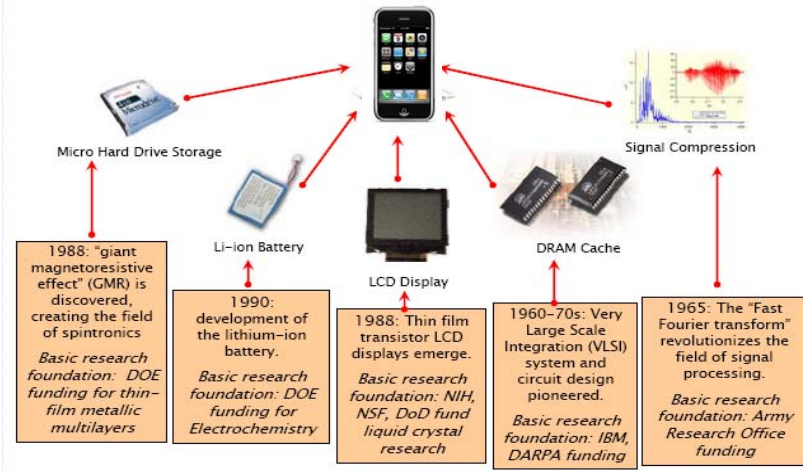
Approximately constant over the last 30 years



The ratio of non-defense science to non-defense discretionary = ~11%

8

Basic Research Impact on Innovation



9

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)

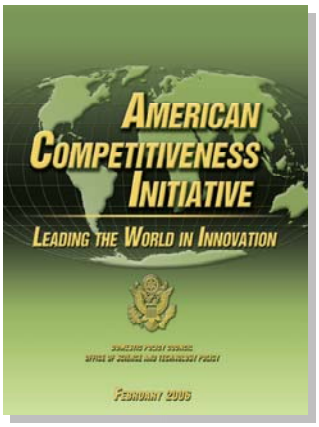
American Competitiveness Initiative

$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

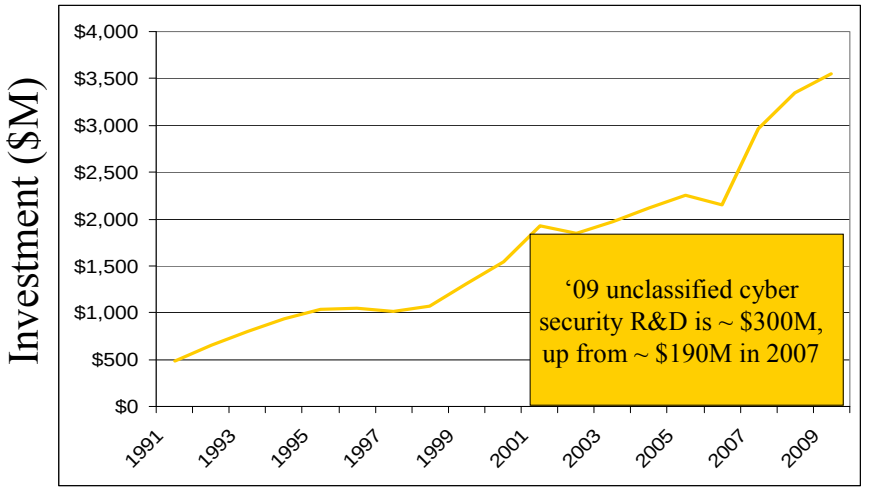
ACI Supports High Impact Research

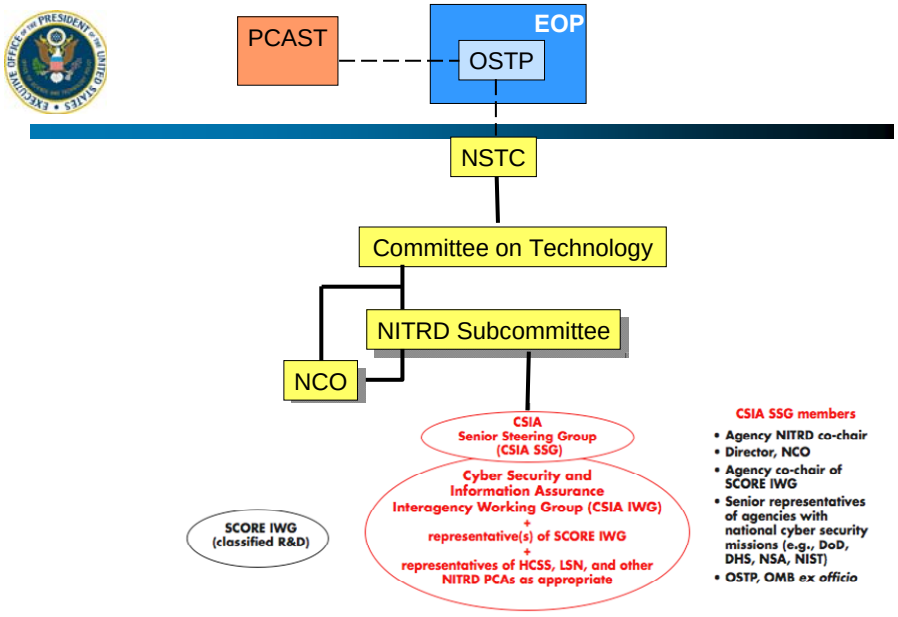


Goals for ACI Research

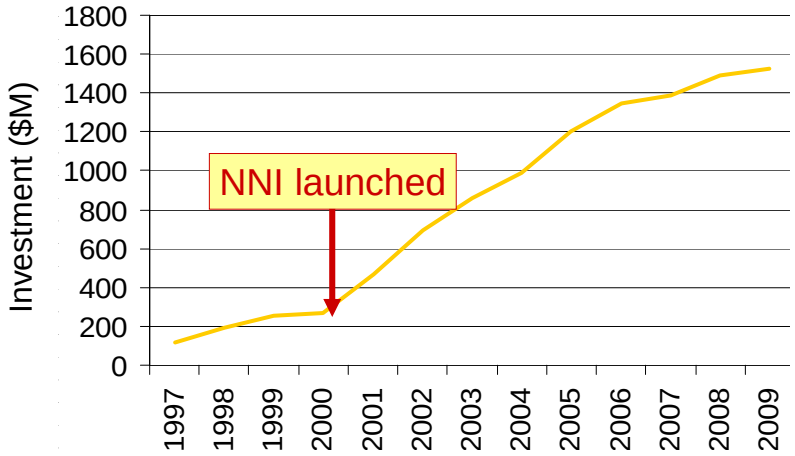
Cyber Security: "Addressing gaps and needs in cyber security and information assurance to protect our IT-dependent economy from both deliberate and unintentional disruption, and to lead the world in intellectual property protection and control"

U.S. Networking and Information Technology R&D Investment

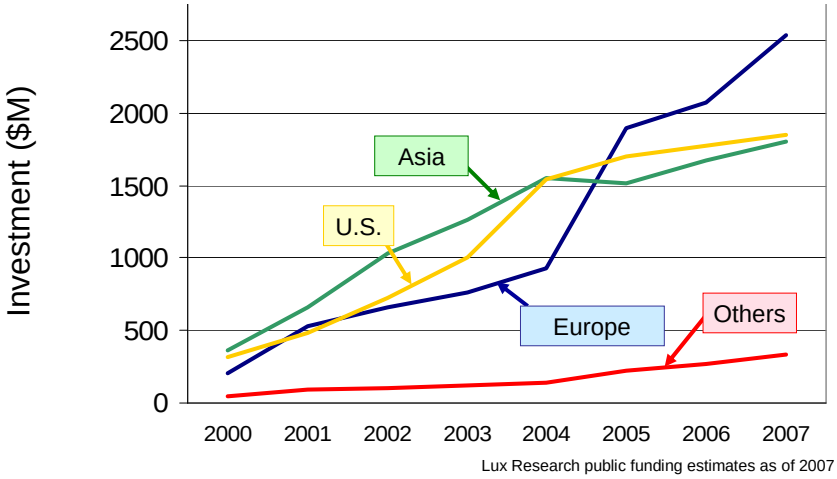




National Nanotechnology Initiative



International Nanotech R&D Investment



APPLICATIONS – Energy Storage

High-Performance Batteries

Identity Management

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

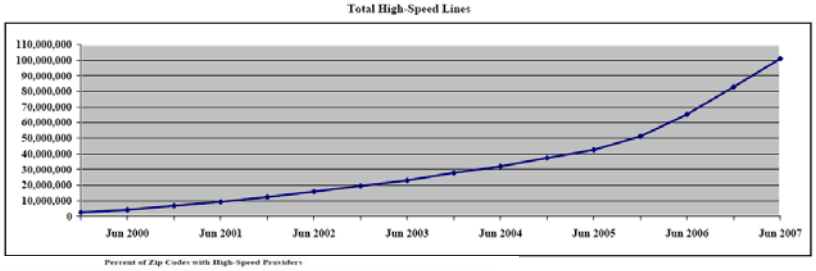
- No normative definition of "Identity Management"
- Governance process required
- Privacy can be enhanced by IdM
- Consolidated IdM vision will enable consistent application of appropriate privacy controls across the IdM landscape
- There will be no "one size fits all" solution – heterogeneous IdM systems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

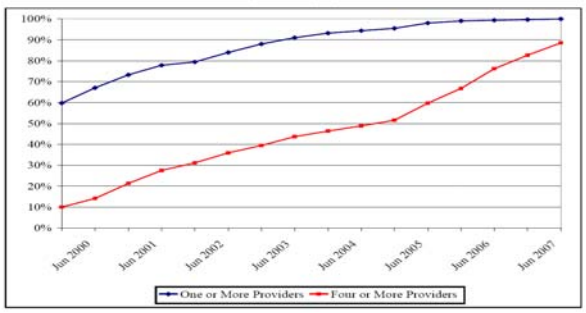
President Bush on Broadband

"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

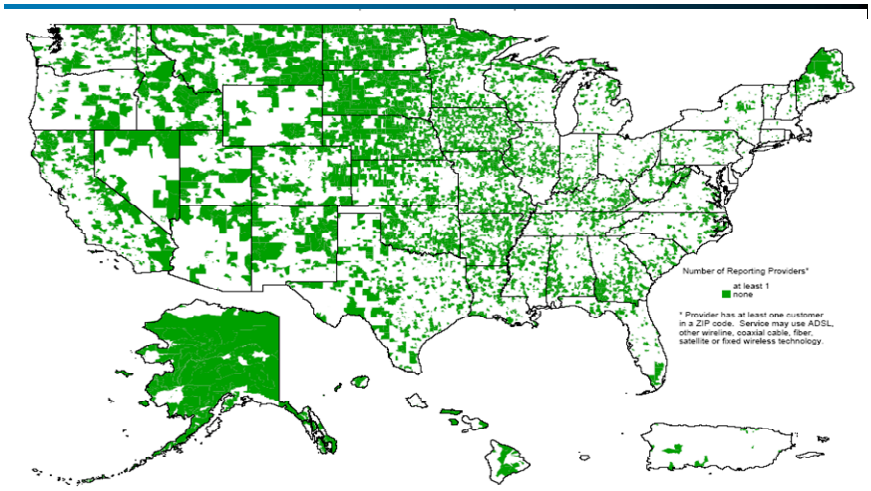




Broadband lines have increased from under 10 million at the start of 2001 to over 100 million lines in June 2007.

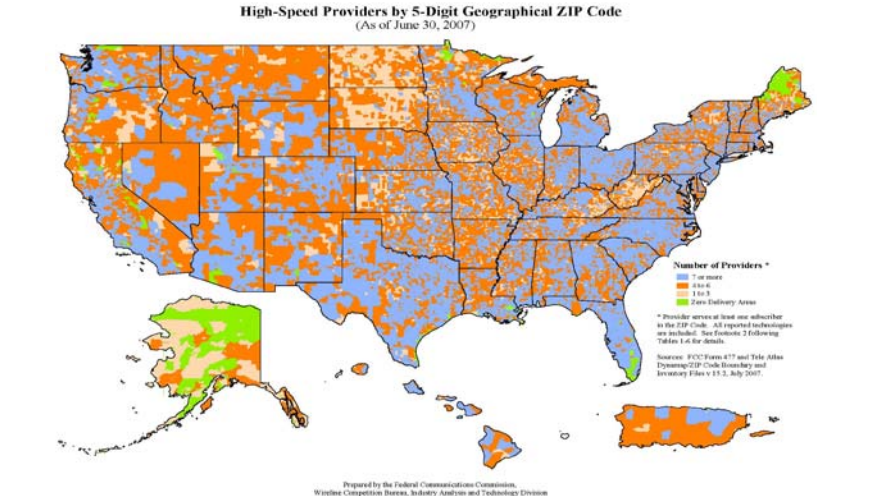
Source: FCC

Broadband Availability by ZIP Code
(As of December 2000)



Green = no broadband

Broadband Availability by ZIP Code
(As of June 2007)



"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***

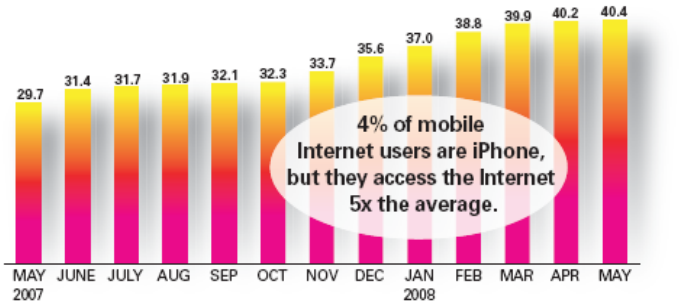
25

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



Source: Nielsen Mobile

APPENDIX D

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

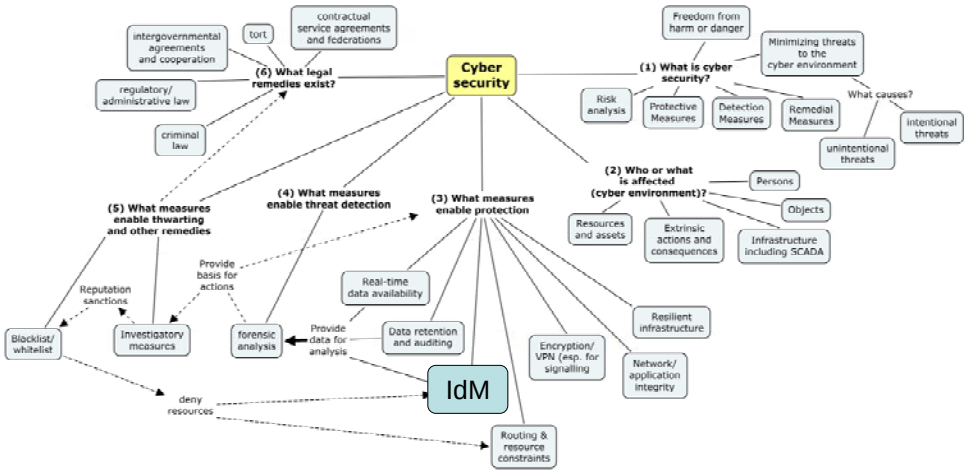
September 26, 2008

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

APPENDIX E

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 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.

APPENDIX F

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