2006 Research and Development Exchange Workshop Proceedings

International Collaboration on Cyber Security Research and Development:

Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response

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

September 21–22, 2006
Ottawa, Ontario, Canada

MEMORANDUM FOR THE INDUSTRY EXECUTIVE SUBCOMMITTEE

SUBJECT: 2006 Research and Development Exchange Workshop Proceedings

On September 21-22, 2006, the Industry Executive Subcommittee's (IES) Research and Development Task Force (RDTF), of the President's National Security Telecommunications Advisory Committee (NSTAC), held its seventh Research and Development Exchange Workshop, at the Crowne Plaza in Ottawa, Ontario, Canada. The purpose of the event was to:

1. Frame key policy issues surrounding international research and development (R&D) collaboration;

2. Explore and prioritize critical issues related to international collaboration on communications and cyber R&D that enhance the preparedness and security of free nations;

3. Provide input to the United States (U.S.) Office of Science and Technology Policy (OSTP), the U.S. Department of Homeland Security (DHS), the U.S. Department of Defense (DOD), the Canadian Department of National Defence (DND), Defence R&D Canada (DRDC), and Industry Canada as they formulate research agendas and budget submissions;

4. Identify and characterize barriers and impediments inhibiting multilateral, collaborative research investments and discuss how international stakeholders can cooperate and capitalize on collective advancements; and

5. Develop an agenda for action.

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 issues affecting communications and cyber networks that enable international collaboration, advance the security of free nations, and enhance preparedness and response activities, including the following: (1) the development of technologies and mechanisms to enable trust and build communities of interest; (2) the importance of international collaboration for the success of cyber security R&D initiatives; (3) the requirement for cost-benefit analyses when making investment decisions for cyber security research; (4) the necessity of dynamic leadership and common frameworks; (5) the need for strengthened education, awareness, and training programs; and (6) the requirement to embed national security and emergency preparedness (NS/EP) requirements in new technologies and methodologies.

The insights, conclusions, and recommendations contained within these Proceedings result from the Workshop and are solely attributable to the combined and unique contributions of 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, Industry Canada, and our breakout session facilitators. In particular, we thank Dr. Anthony Ashley, Director General, DRDC Ottawa; Mr. John Grimes, Assistant Secretary for Networks and Information Integration and Chief Information Officer, DOD; Dr. Veena Rawat, President, Communications Research Centre Canada; Ms. Patricia Sauvé-McCuan, Assistant Deputy Minister, Information Management, DND; Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, DHS; and Mr. Michael Zafirovski, Chairman and Chief Executive Officer, Nortel, for their personal engagement in the event, which greatly contributed to its success. We also acknowledge the important contributions from Dr. Annabelle Lee, Section Director, Security Standards, National Cyber Security Division, DHS; Dr. Douglas Maughan, Program Manager, Cyber Security R&D, DHS; and Dr. Simon Szykman, Director, National Coordinating Office for Networking and Information Technology R&D. We are also grateful to the staff's outstanding performance in their attention to so many details. Finally, we extend many thanks to the NSTAC member companies for their resources and support.

Respectfully,

Guy L. Copeland, Computer Sciences Corporation
Chair, Research and Development Task Force

ACKNOWLEDGEMENTS

The Research and Development Task Force of the President's National Security Telecommunications Advisory Committee would like to thank the representatives from industry, Government, and academia who participated in the first ever International Research and Development Exchange (RDX) Workshop held at the Crowne Plaza on September 21-22, 2006, in Ottawa, Ontario, Canada. The RDTF would especially like to acknowledge the important contributions of the Department of Defense (DOD), the Department of Homeland Security (DHS), the Department of National Defence (DND), Industry Canada, and the Office of the Manager, National Communications System (NCS) for the planning and execution of the 2006 RDX Workshop.

A special thanks to the Workshop Moderators, Mr. John Grimes, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, DOD; Ms. Patricia Sauvé-McCuan, Assistant Deputy Minister, Information Management, DND; and our invited speakers, Dr. Anthony Ashley, Director General, Centre for Security Science, Defense Research and Development Canada (DRDC) Ottawa; Dr. Peter Fonash, Deputy Manager, NCS, DHS; Dr. Annabelle Lee, Section Director, Security Standards, National Cyber Security Division, DHS; Dr. Douglas Maughan, Program Manager for Cyber Security Research and Development (R&D), Homeland Security Advanced Research Projects Agency, Science and Technology Directorate, DHS; Dr. Veena Rawat, President, Communications Research Centre Canada; Mr. John Roese, Chief Technology Officer, Nortel; Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, DHS; Dr. Simon Szykman, Director, National Coordinating Office for Networking and Information Technology R&D; and Mr. Michael Zafirovski, President and Chief Executive Officer, Nortel.

We would also like to extend our sincere appreciation to our breakout session co-facilitators, Mr. Michael Alagna, Motorola; Mr. Stuart Brindley, Independent Electricity System Operator; Mr. Jim Brookes, Mathematics of Information Technology and Complex Systems; Mr. Reg Foulkes, Computer Sciences Corporation Canada; Dr. Seymour Goodman, Georgia Institute of Technology; Dr. Julie Lefebvre, DRDC Ottawa; Dr. Jack Oslund, George Washington University; Dr. Tim Moses, Entrust; Mr. Marcus Sachs, SRI International; and Mr. Rod Wallace, Nortel.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

From September 21–22, 2006, the President's National Security Telecommunications Advisory Committee (NSTAC) conducted its seventh Research and Development Exchange (RDX) Workshop entitled, *International Collaboration on Cyber Security Research and Development: Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response*. 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 communications and cyber networks that enable international collaboration, 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 way national security and emergency preparedness (NS/EP) communications are planned for, prioritized, and ultimately delivered. The 2006 RDX Workshop addressed the need for multilateral collaboration between key Governments, industry, and academia to enhance security on the network. Specifically, international stakeholders from these three sectors were invited to explore and prioritize issues associated with international collaboration on cyber security R&D.

The goal of the event was to gather valuable information and constructive feedback, which will inform the Research and Development Task Force as it develops proposed Presidential recommendations for the NSTAC. The R&D community's feedback will assist the task force in: (1) framing key policy issues surrounding international R&D collaboration; (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, Department of Homeland Security, Department of Defense (DOD), Department of National Defence (DND), Industry Canada, and other key international stakeholders as they formulate research agendas and budget submissions; (4) identify and characterize barriers and impediments inhibiting multilateral, collaborative research investments; and (5) develop an agenda for action.

Specifically, the event examined five focused topics:

- **International Internet Governance**: Effectively managing the technologically complex global communication network and strengthening the security and stability of the Internet.

- **Global-Scale Identity Management**: Identifying and authenticating people, hardware devices, and software applications when accessing critical and sensitive information technology (IT) systems.

- **Collaborative Mechanisms for Network Security Protocol R&D**: Promoting public/private partnership mechanisms to foster stable investment in R&D for network security protocols, thereby enhancing the resiliency of communications and cyber networks.

- **Cross-Border and Cross-Sector Challenges**: Establishing a cross-sector and cross-border approach that examines impediments to international cooperation and governance mechanisms and focuses on development of a deployment strategy to address infrastructure interdependencies before they are highlighted during a cross-border disaster.

- **Wireless and Mobile Ad Hoc Applications**: Ensuring technical stability, security, and efficient management of wireless and mobile ad hoc networks employed during times of national crisis or natural disaster.

During the two-day event, participants engaged in a facilitated dialogue including both plenary and breakout sessions. From these sessions, six overarching issue areas and corresponding agendas for action regarding international collaboration for cyber security R&D emerged:

- **Technologies and mechanisms to enable trust and build communities of interest are needed.** Enhanced security on the global communications network is dependent on an ability to interpret the trustworthiness of infrastructure, users, and devices. Several factors, such as human error, the need for commercial efficiencies, effective security policies and procedures, and personnel security and background checks, influence how trust is embedded in systems. The current network environment lacks universal applications and exercised processes and practices that allow parties to establish a high degree of confidence in the legitimacy and reliability of their counterparts, thereby stifling the development of functional communities of interest. Confidence and trust are jeopardized by a host of threats (such as exploitation by insiders, physical destruction). To enable inter-domain trust, users and devices must be able to develop, transfer, and accept identities and credentials through systems and solutions that provide for cross-recognition.

- **International collaboration is essential for successful cyber security R&D initiatives.** Current collaboration is limited and localized. R&D partnerships need to be created to promote cooperation and interoperation across borders, infrastructures, sectors, and domains. To effectively address the compelling network security risks that threaten economic sustainability, national security, and public safety, information sharing forums and mechanisms are essential for exchanging information and conducting collaborative R&D activities are imperative. Legislative and regulatory barriers need to be amended and incentives need to be created to facilitate appropriate levels of information sharing and international cooperation.

- **To advance cyber security research, leaders and practitioners must make investment decisions based on cost benefit analyses.** Recent innovations and advancements in networked information systems have brought about dynamic change, driven primarily by commercial forces. However, the security paradigm has not shifted to accommodate this evolving environment, thereby thwarting long-term progress. Future cyber security R&D proposals must address the cost of collaboration, articulate the value proposition, and include relevant business cases. To accomplish a posture of improved security and trustworthiness, strategies should be devised to leverage industry investments while accommodating market drivers; balance directives and incentives to stimulate progress; and blend influence and action to develop the next generation of security tools and products.

- **To maintain the current security posture and improve future preparedness and response, NS/EP requirements must be embedded in new technologies and methodologies.** The rapid pace of technological advancement demands increased focused on the importance of ensuring the resiliency, reliability and security of critical communications. Additional research on NS/EP scenarios and requirements is needed, as well as further development of existing systems and technologies that may have NS/EP applications. Future cyber security R&D must also consider how potential market decisions and economic impacts affect the security of free nations. New tools and services must incorporate NS/EP requirements during the pre-R&D stages and must continue to consider NS/EP implications through technology deployment and commercial adaptation.

- **Dynamic leadership and common frameworks are critical to achieve real progress in cyber security R&D.** General agreement on the set of "grand challenges" is needed to achieve larger goals and to encourage cross-border and cross-sector partnerships. Such vision serves to encourage collaboration, justify expenditures, and build global communities of interest around cyber security R&D. In addition, a common taxonomy enables different parties to clearly define priorities. While multinational standards efforts facilitate the development of common frameworks, cross-sector agreement on a roadmap for future R&D expenditures is also vital.

- **Strengthened education, awareness, and training programs increase the effectiveness of R&D partnerships and programs.** By improving knowledge sharing, members of the research community will be able to leverage best practices and related initiatives to enhance the effectiveness of current and future R&D investments. The critical challenge is to develop an R&D strategy that engages industry, Government, and academia, as well as end-users in exchanging information about existing initiatives and successes, thereby ensuring consideration of the full range of critical issues and facilitating the development of comprehensive, holistic solutions collectively. To inform the development of requirements and priorities, it is necessary to maintain an inventory of ongoing activities and to create linkages between centers of excellence across the world.

During the plenary closing session, Mr. John Grimes, Assistant Secretary for Defense, Network and Information Integration and Chief Information Office, DOD and Ms. Patricia Sauvé-McCuan, Assistant Deputy Minister, Information Management, DND challenged the five breakout session groups to closely examine identified research priorities and consider how they can be expanded to enhance military operations.

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 (NS/EP) telecommunications issues. From September 21–22, 2006, the RDTF conducted its seventh Research and Development Exchange (RDX) Workshop entitled, *International Collaboration on Cyber Security Research and Development: Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response*.

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 (NGN) will revolutionize the way NS/EP communications are planned for, prioritized, and ultimately delivered. Given this evolving market and technology environment, the Workshop addressed the need for collaboration to preserve and enhance network security through targeted R&D approaches. The two-day event featured keynote speakers and breakout sessions focused on the full range of cyber security research and development (R&D) issues associated with advancing the security of free nations and enhancing preparedness and response activities across sectors. Specifically, international stakeholders explored five different issues associated with international collaboration on cyber security R&D:

- **International Internet Governance**: Effectively managing the technologically complex global communication network and strengthening the security and stability of the Internet.

- **Global-Scale Identity Management**: Identifying and authenticating people, hardware devices, and software applications when accessing critical and sensitive information technology (IT) systems and NGN.

- **Collaborative Mechanisms for Network Security Protocol R&D**: Promoting public/private partnership mechanisms to foster stable investment in R&D for network security protocols, thereby enhancing the resiliency of communications and cyber networks.

- **Cross-Border and Cross-Sector Challenges**: Establishing a cross-sector and cross-border approach that examines impediments to international cooperation and governance mechanisms and focuses on development of a deployment strategy to address infrastructure interdependencies before they are highlighted during a cross-border disaster.

- **Wireless and Mobile Ad Hoc Applications**: Ensuring technical stability, security, and efficient management of wireless and mobile ad hoc networks employed during times of national crisis or natural disaster.

1.2 Purpose

The RDX Workshop strengthened cross-border collaboration and facilitated an exchange of ideas among researchers and practitioners from academia, industry, and Government on critical issues related to international collaboration on cyber security. To stimulate robust discussion, facilitators and participants from the vendor, network provider, academic, and Government communities were invited to attend to present their viewpoints. The event gathered valuable information and constructive feedback, which will provide input to budgetary decisions and research agendas and inform the RDTF as it develops proposed Presidential recommendations for the NSTAC.

1.3 Proceedings Organization

This Proceedings document provides an overview of the 2006 RDX Workshop. Specifically, it is divided into six sections and associated appendices:

- Section 1 presents background information on the 2006 RDX Workshop;
- Section 2 reviews the opening plenary session, including:
    - Welcoming remarks from Mr. Guy Copeland, Computer Sciences Corporation (CSC) and RDTF Chair, and Mr. John Roese, Chief Technology Officer (CTO), Nortel;
    - Addresses delivered by the co-moderators, Mr. John Grimes, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, Department of Defense, and Ms. Patricia Sauvé-McCuan, Assistant Deputy Minister, Information Management, Department of National Defence (DND); and
    - Remarks and presentations from Dr. Anthony Ashley, Director General, Defence R&D Canada (DRDC) Ottawa; Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, Department of Homeland Security (DHS); Dr. Douglas Maughan, Program Manager, Homeland Security Advanced Research Projects Agency (HSARPA), DHS; Dr. Annabelle Lee, Section Director, National Cyber Security Division (NCSD), DHS; and Dr. Simon Szykman, Director, National Coordinating Office (NCO) for Networking and IT R&D (NITRD).
- Section 3 summarizes the luncheon addresses from Mr. Michael Zafirovski, President and Chief Executive Officer (CEO), Nortel and Dr. Veena Rawat, Communications Research Centre (CRC) Canada;

- Section 4 captures the observations and findings from the breakout sessions;
- Section 5 highlights discussions from the closing plenary session;
- Section 6 presents the major findings from the 2006 RDX Workshop; and
- Appendices A–F include the RDX Workshop agenda, speakers' prepared remarks, speaker and facilitator biographies, and other materials.

2.0 OPENING PLENARY SESSION

The opening plenary session to the 2006 RDX Workshop commenced with remarks from Mr. Guy Copland, CSC and RDTF Chair. Mr. Copeland welcomed participants and noted the importance of the first-ever international RDX Workshop, with participants from the United States (U.S.), Canada, and the United Kingdom. He emphasized the need to address international collaboration on the full range of communications and cyber security R&D issues that advance the security of free nations and enhance preparedness and response activities across sectors. Mr. Copeland thanked participants for their attendance and encouraged them to focus discussions on providing actionable recommendations that can be implemented by key decision makers concerned with improving security, preparedness, and response efforts both within and across borders.

Mr. Copeland reviewed the agenda and format for the event and made several administrative announcements. Next, he briefly described the history of the NSTAC's involvement in the 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 telecommunications. He then described the objectives for the 2006 RDX Workshop, commenting that breakout session groups would: (1) explore and prioritize critical R&D requirements for international collaboration; (2) frame key policy issues related to coordinating international initiatives; and (3) identify and characterize barriers and impediments inhibiting multilateral, collaborative research investments. Mr. Copeland concluded by reiterating the need for developing actionable recommendations for key stakeholders to carry forward.

2.1 Welcoming Remarks—Mr. John Roese

Mr. Copeland introduced Mr. Roese, CTO, Nortel. Mr. Roese welcomed participants to the city of Ottawa and briefly described his background at Nortel. He then discussed the changing landscape of the communications industry, noting the increasing emphasis on security considerations in communications system design. Mr. Roese also noted the importance of identity and authentication within the communications network, as these issues are becoming fundamental pillars in decision making.

Mr. Roese continued by engaging participants in thoughts around the question, "What keeps you up at night?" He described his fears of the combination of an intelligent hacker community and an unsecured communications infrastructure. Mr. Roese concluded his thoughts by highlighting the urgent need for participants to discuss a strategy for appropriate identity and authentication to ensure a secure network in the future.

2.2 Moderator's Address—Ms. Patricia Sauvé-McCuan

Mr. Roese introduced Ms. Patricia Sauvé-McCuan, Assistant Deputy Minister, Information Management, DND, and Ms. Sauvé-McCuan expressed her appreciation for the opportunity to address the group and noted that the RDX Workshop is representative of the strong collaboration between allied nations. Ms. Sauvé-McCuan emphasized the criticality of working together to

ensure robust and secure technological platforms, noting that partnerships between nations are essential in light of the threat of cyber terrorism and the absence of borders to information flow over the Internet. To illustrate the threat, Ms. Sauvé-McCuan described a hypothetical scenario involving a power failure in Toronto, Canada that causes sporadic disruptions to the Toronto subway system, thereby impacting supporting businesses. The connections between the disruptions and their effects are not realized for several weeks, and the power failure ultimately results in a significant economic impact. In this case, a power failure ultimately impacted the networks controlling the subway system and supporting businesses, which demonstrates that a cyber attack can take many forms.

Ms. Sauvé-McCuan recognized that since the advent of the Internet roughly 40 years ago, the dream of business connectivity has been realized, and the world's developing nations are achieving 50 percent connectivity. However, in the development stages of the Internet, it was never imagined that the very tool that would connect businesses could also be used to attack businesses, the economy, and enable criminals to steal the identities of others. The world is now faced with the challenge of ensuring a safe and secure cyber world.

Ms. Sauvé-McCuan highlighted several challenges in securing the Internet. First, she noted the global nature of cyber security and the interconnectedness of the networks and emphasized that currently, the only truly secure networks are closed access military networks, which are not connected to the global infrastructure. She explained that there is an inherent challenge in ensuring the availability and security of the network while remaining globally connected. Furthermore, Ms. Sauvé-McCuan emphasized that current trends indicate that increasingly destructive attacks are likely to occur on the Internet, and informed the participants that the frequency, speed, and complexity of attacks are increasing exponentially. To address this challenge, the Canadian Government has formed a Cyber Security Task Force to strengthen its capabilities to protect the Internet. Second, she noted that responsibility for cyber security belongs to the owners and operators of the infrastructure; however, the Government has a responsibility to educate the owners and operators on how to best secure the infrastructure. Such education and advice can come in the form of Government-mandated standards. Third, she reminded the participants that there is a need to determine the appropriate legislative framework for cyber security, which should balance civil rights and security needs. Fourth, she stated that since cyber security is a global issue, secure global information sharing mechanisms are needed.

Ms. Sauvé-McCuan discussed several areas of focus that should be included in research efforts. Specifically, efforts should include an analysis of all new cyber security tools and capabilities to help ensure improved allocation of resources. In addition, the interdependencies between sectors should be recognized and she suggested that new protection solutions should be developed to help secure other vulnerable infrastructures.

(Note: The full text of Ms. Sauve-McCuan's moderator's address is attached in Appendix C)

2.3 Moderator's Address—Mr. John Grimes

Mr. Copeland introduced Mr. Grimes, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, DOD. Mr. Grimes expressed his appreciation for the work of the President's NSTAC. He noted that the success of the NSTAC is

rooted in the genuine industry/Government partnership that the NSTAC exemplifies. Throughout its 25-year history, the NSTAC has evolved with both technological advancements and changing national priorities. Initially, the NSTAC focused its efforts on NS/EP issues associated with traditional telephony. The first meeting of the NSTAC was chaired by President Ronald Reagan, who, during that meeting, emphasized the Government's dependence on industry for ensuring reliable and secure communications. However, the security and technological environment has evolved since that initial meeting, and today it is clear that the Government is not only dependent on industry for secure communications, but, with convergence to the NGN, will increasingly need to engage in international partnerships. Furthermore, the work of the NSTAC has recently focused significant efforts on timely issues such as disaster recovery.

Mr. Grimes illustrated how he has seen national priorities evolve over the years. During his tenure on the Defense Science Board, priorities were more cultural than technological in nature. At that time, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* had recently passed, which led to increased cross-cutting of cultural and technological issues. Specifically, information sharing grew to be the primary issue of concern. Today, as technologies have evolved, so have the concerns, and attention is shifting to issues such as international Internet governance. In addition, communications and IT concerns are beginning to not only cross national borders, but are also cutting across the infrastructure sectors. Furthermore, for first responders and warfighters in the field, spectrum allocation is growing increasingly important and significant R&D is currently underway regarding the development of compliant radios for intelligence purposes. In addition, DOD is focusing on net-centricity.

Mr. Grimes further elaborated on those issues that "keep him up at night." He noted that the threat to the communications infrastructure is very real and the capabilities of adversaries are growing more sophisticated everyday. DOD has an approximately $30 billion IT budget, with a significant amount of this funding dedicated to protecting their network. He is concerned about the vulnerabilities created by the outsourcing of software development for weapons systems and the sharing of servers and routers for both the electric power and financial sectors. To combat some of these vulnerabilities, he noted that DOD currently has significant identity management and biometrics efforts underway. Mr. Grimes assured the participants that these concerns have been brought to the attention of the President, who has received a number of briefings on the vulnerabilities of the Nation's networks. Furthermore, Secretary Donald Rumsfeld, DOD, is well aware of these vulnerabilities and understands the linkage to national defense mechanisms, including the net-centric systems upon which the Nation's warfighters depend. Mr. Grimes also noted that the North Atlantic Treaty Organization has recently enabled a capability similar to DOD's net-centricity operating model.

Mr. Grimes then described a framework for the future network strategy that includes cross-domain information sharing, enterprise services, cooperative engagement, and information transport. Specifically, he noted the growing importance of net-centricity and the need to consider industry's direction in the next ten years to ensure that R&D funding is not spent in areas that will soon be obsolete.

Mr. Grimes then responded to questions from the participants. A question was raised regarding current international collaboration for cyber security. Mr. Grimes noted that the World Summit on the Information Society recently met in Tunis, Tunisia and has been working hard to develop some multilateral agreements among nations.

2.4 Canadian Public Security Science and Technology Program: A Look to the Future—Dr. Anthony Ashley

Mr. Roese introduced Dr. Anthony Ashley, Director General, DRDC Ottawa. Dr. Ashley opened his remarks by describing the cyber security R&D component of the science and technology (S&T) program with which he is currently involved. He emphasized the need to examine cyber security R&D from an international perspective. Dr. Ashley then focused on the range of initiatives established by the Government since the September 11, 2001, terrorist attacks, such as exercises and cyber security task forces. He finished his introductory statement by highlighting that S&T are key enablers for these initiatives.

Dr. Ashley noted the importance of security work based on the known impact of recent events and further described the initiatives currently underway in support of the Canadian Public Safety and Security Strategy. Among them, he specifically called out *Securing an Open Society: Canada's National Security Policy;* the *National Chemical, Biological, Radiological, and Nuclear (CBRN) Strategy of the Government of Canada*; the National Exercise Plan; and Canada's Cyber Security Task Force. Dr. Ashley continued by describing the Public Security S&T Program, which is a treaty-level agreement that brings R&D together for both the U.S. and Canada. The Public Security S&T Program supports mechanisms to co-fund R&D projects between both nations. Dr. Ashley then highlighted that the main goal for this initiative is for the U.S. and Canada to develop a collaborative S&T program to facilitate better information sharing mechanisms.

Dr. Ashley also described the CBRN Research and Technology Initiative (CRTI). He noted the importance of this initiative and indicated that its mission focuses on strengthening Canada's preparedness for, prevention of, and response to a CBRN terrorist attack through new investments in science, research, and technology capacity. Dr. Ashley described several model implementations through CRTI, including the development of a risk assessment process, a research and technology program, a technology acceleration project, and a technology demonstration program. These programs are mechanisms that allow senior Government officials to lead discussions in their respective communities. Within the CRTI, Dr. Ashley described several accomplishments. Currently, the risk assessment approach is the hallmark of the program. In addition, Dr. Ashley explained the importance of information sharing concepts developed through the CRTI and noted that a portal is needed to share information among the Federal, State, and municipal levels. Dr. Ashley described the focus of current CRTI projects, including protection in harsh environments, event detection, triage to monitor the consequences of an event, and remediation. He highlighted the importance of these items and emphasized the need to bring the processes into all cyber security projects.

Dr. Ashley continued by introducing the Centre for Security Science, which was developed based on recognition of the need to expand from the CBRN domain. The Centre for Security Science is jointly sponsored by Public Safety and Emergency Preparedness Canada and DRDC

and currently sponsors several S&T programs with a range of partners and clients. Dr. Ashley described the international activities within the Centre for Security Science, including a Canadian/U.S. Public Security Technical Program (PSTP) bilateral, and Canadian/U.S. Security and Prosperity Partnership Goal 10. He further noted that all initiatives are focused on industry and academia outreach.

Dr. Ashley then introduced the Canadian PSTP, which is built upon the solid CRTI program foundation and directly supports the Canadian/U.S. PSTP bilateral program. He further described the mission of the program, which expands to an 'all hazards' approach to address critical infrastructure protection by including terrorism, criminal intent, natural disasters, and accidental technical disasters. Dr. Ashley explained that the Canadian PSTP is focused on five mission critical outcomes: (1) focusing public safety and security policy towards a national capability; (2) developing a national emergency management system to ensure the capability is in place and responsive; (3) ensuring a robust national surveillance and intelligence gathering, analysis, and dissemination for rapid intervention during events; (4) guaranteeing rapid identification of critical infrastructure vulnerabilities to achieve enhanced all hazards robustness; and (5) developing national capabilities to ensure safe, secure, and efficient flow of people, goods, and services across borders and ports of entry. In addressing the mission critical outcomes, Dr. Ashley identified several focused enablers, including affordable technologies, national standards for interoperability, protocols for information sharing, integrated risk assessments, and models to support decision-making techniques.

Dr. Ashley continued by describing several portfolios under the Canadian PSTP. He began by explaining the chemical, biological, radiological, nuclear, and explosives (CBRNE) portfolio, which focuses on developing capabilities to prevent, prepare for, and respond to CBRNE threats to public security, whether derived from terrorist or criminal activity, natural causes, or accidents. Dr. Ashley also described the Disruption and Interdiction initiative, focused on the ability to identify and stop terrorists and their activities, including surveillance, monitoring, disruption, and interdiction of their activities, as pertaining to border and transportation security. In addition, Dr. Ashley highlighted the Systems Integration, Standards, and Analysis (SISA) portfolio. He noted that SISA is mainly focused on interoperability issues. Its mission focuses on the performance, integration, and interoperability of national and international public security and emergency management capabilities and supporting systems, including the enabling standards, and vulnerability and systems analyses.

Dr. Ashley also described the Cyber Critical Infrastructure Protection (CIP) Program. He noted the pervasiveness of computers in modern society, highlighting that they are often the cornerstone for a majority of the critical infrastructures, which clarifies the need for CIP in the communications infrastructure and cyber security mechanisms. Dr. Ashley explained that the Cyber CIP Program is now focused on determining the road ahead for cyber security. In this context, the Cyber CIP Program sponsored a prospective futures workshop to look ahead to possible cyber CIP challenges in 2015. Dr. Ashley noted that the workshop produced several conclusions, including continued rapid growth of wireless networks and associated security issues, continued growth in the complexity of private networks and sub-networks with increasingly distributed ownership, and the introduction of quantum computing, which will likely render normal cryptographic keys useless.

Dr. Ashley concluded his keynote address by describing a summary of the future of cyber security. He described a proposal to develop a committee of industry, Government, and academia to focus on the identification of cyber security vulnerabilities. He also highlighted the importance of the 2006 RDX Workshop within this context. Dr. Ashley concluded by emphasizing the need for international collaboration among the U.S., Canada, and other nations. Mr. Copeland thanked Dr. Ashley for his address and involvement in the 2006 RDX Workshop.

2.5 Meeting Security Challenges of the 21st Century Risk Environment—Mr. Robert Stephan

Mr. Copeland introduced Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, DHS. Mr. Stephan began his remarks by characterizing the 21st century risk environment in terms of the growing threat to and vulnerabilities of increasingly interconnected critical infrastructures. Mr. Stephan stated that today's threat is significant, ubiquitous, and multidimensional, encompassing both physical and cyber components. The cyber threat includes a comprehensive spectrum of cyber perpetrators, ranging from high school hackers to criminal organizations and nation state sponsors. The threat continues to change and adapt in both physical and cyber aspects in response to application of mitigation strategies. Mr. Stephan described the unique threat that international terrorism poses to civilized nations, noting that, like private and public sector organizations, terrorist groups also develop and exploit aggressive R&D and S&T components, and will use any means necessary to achieve their objectives.

Mr. Stephan reported that systems across all 17 critical infrastructure sectors continue to be vulnerable to both physical and cyber threats. While intrinsic vulnerabilities exist due to interconnectedness between the sectors, more emphasis should be placed on addressing the security open access systems in all sectors. Mr. Stephan also noted that all critical infrastructure sectors depend on the telecommunications and electric power (EP) infrastructures and attacks on such infrastructure assets could have regional, national, and international impacts and result in cross-sector cascading effects.

Shifting his focus to protection strategies, Mr. Stephan observed that a number of factors impede the ability to effectively respond to the threat on a nationwide level. Achieving a focused command and control environment to enable protection is difficult given the involvement of myriad Federal, State, and local Government stakeholders. He stated that strategies must also balance the Nation's abiding respect for individual freedoms and privacy rights. Effective solutions necessarily will engage an integrated network of authorities and capabilities across multiple sectors and jurisdictions.

Mr. Stephan then identified and commented on three keys to success in meeting the challenges posed by the 21st century risk environment: (1) leadership; (2) partnership; and (3) planning. First, Mr. Stephan commented that decisive leadership is required at all Government levels. Leaders must recognize the problem, apply a holistic approach, and ensure a suitable commitment of resources. He stated that the leadership commitment exists within DOD and DHS and progress continues to be catalogued regarding organizing and governance structures, strategic planning, information sharing mechanisms, and cooperative frameworks, such as the Security and Prosperity Partnership of North America.

Second, Mr. Stephan stated that establishing and enhancing partnerships are critical, both among and between responsible private and public sector organizations. He noted that existing partnerships vary in maturity across the sectors and ongoing successful partnership models, such as the NSTAC, continue to be leveraged to enhance public/private sector collaboration and information sharing.

Third, Mr. Stephan emphasized the importance of effective planning, and as a case in point, described development of the National Infrastructure Protection Plan (NIPP). The NIPP was developed through a successful public/private partnership across all levels of Government, including unofficial review and input from the Canadian Government. He explained that the NIPP provides a coordinated approach to critical infrastructure and key resource protection roles and responsibilities for Federal, State, local, tribal, and private sector security partners. He commended the progress made to date, noting development of individual sector plans or "mini-NIPPs," ongoing actions to build physical and cyber security components into each sector plan, and incorporation of a NIPP chapter that specifically addresses R&D planning. Mr. Stephan also encouraged efforts to proactively build defenses into system front ends, recognizing that the increasing threat continues to compress required response timeframes.

Mr. Stephan continued his address by identifying specific focus areas that require critical attention of policy makers and R&D practitioners:

- Surveillance and intrusion detection systems;
- Approaches to "home-made" devices such as liquid explosives;
- Time-sensitive decision support systems that can rapidly inform decision makers;
- Horizontal and vertical information sharing systems and mechanisms to ensure effective sharing across communities of interest;
- Approaches to building resiliency into systems and realizing the full potential of self-healing networks/infrastructures; and
- Control system protections to include Supervisory Control and Data Acquisition (SCADA) system support.

Recognizing that a significant coordinated and disciplined effort is needed to address these and other focus areas, Mr. Stephan advised continued use of established processes, such as the NSTAC, to propose recommendations and establish policy priorities. He continued by highlighting the important role that both industry and Government stakeholders play in prioritizing R&D requirements for Government action and resource allocation, and recommended use of the NIPP process and the Sector Coordinating Councils (SCC) to surface R&D requirements. Mr. Stephan stated that the DHS S&T Directorate has made considerable progress, noting that its recent reorganization recognizes the importance of cyber R&D and the need for actual mission requirements to drive the cyber R&D agenda.

Mr. Stephan concluded his remarks by acknowledging the extremely high stakes presented by the current wartime risk environment, noting that an incident such as detonation of a weapon of mass destruction would forever change the existing landscape. He counseled continued vigilance and solicited the assistance of all participants in leveraging their combined talent and initiative to focus on the critical issues and counter the continuing threat.

2.6 Cyber Security R&D Initiatives at the Department of Homeland Security—Dr. Douglas Maughan

Mr. Copeland introduced Dr. Doug Maughan, Program Manager for Cyber Security R&D, HSARPA, S&T Directorate, DHS. Dr. Maughan began his presentation by describing the mission of the S&T Directorate, which is focused on development, test, evaluation, and commercialization, as opposed to the Defense Advanced Research and Projects Agency or the National Security Administration, which are concentrated on basic research. However, the newly confirmed Under Secretary for S&T, Rear Admiral Jay Cohen, would like to focus more on basic research. HSARPA engages the private sector to meet operational homeland security requirements, conduct prototyping and commercial adaptation, and R&D revolutionary options.

Dr. Maughan noted that he runs the Cyber Security R&D Center, which is managed and staffed by SRI International. He described its R&D execution model, which seeks collaboration and input from Federal Government customers and critical infrastructure providers to prioritize requirements. Then, the Center consults sector roadmaps, holds workshops, and prepares solicitations. In the next phase, the Center feeds the R&D portfolio through various mechanisms, including its major program areas, broad agency announcements (BAA), small business innovative research (SBIR), and supporting programs. Finally, it follows up these initiatives with experiments and exercises, coordination with industry and Government, and outreach activities. The major cyber security program areas are information infrastructure security, research tools and techniques, next generation technologies, and other activities including emerging threats and rapid technology and prototyping (RTAP).

The Information Infrastructure Security (IIS) Program within the Cyber Security R&D Center was formed in response to the President's *National Strategy to Secure Cyberspace* to encourage the adoption of improved security protocols, such as Domain Name System Security (DNSSEC) and Secure Border Gateway Protocol (BGP). The IIS Program is composed of two major sub-programs: the DNSSEC initiative and the Secure Protocols for the Routing Infrastructure (SPRI) project. The DNSSEC initiative helps to meet the requirements of the *Federal Information Security Management Act*, which mandates the deployment of DNSSEC. DHS is involved in a number of different activities as a part of the DNSSEC initiative including roadmap development, multiple workshops, a National Institute of Standards and Technology (NIST) testbed, a publicity and awareness plan, development of policy and technical guidance, and deployment pilots. The SPRI project addresses the vulnerability of the BGP architecture and develops solutions for current routing security problems and future technologies. Through the SPRI project, DHS cleans up existing data in registries and legacy address spaces; employs public key infrastructures between naming authorities, registries, service providers, and customers; and identifies remaining R&D to improve tools for secure routing management.

The Center's Cyber Security Research Tools and Techniques Program tests next generation cyber security through the joint DHS and National Science Foundation Cyber Security Testbed and the Protected Repository for Defense of Infrastructure against Cyber Threats (PREDICT). The testbed currently includes 350 nodes and will be expanded to 1000 nodes across six sites. The experimental infrastructure is open, vendor-neutral, and free for use by researchers. The PREDICT program aims to improve the quality of defensive cyber security technologies through the production of datasets for testing and the evaluation of maturing networking technologies.

Data collection activities provide classes of data from real networks that are of interest to the research community.

The Experiments and Exercises Program within the DHS Cyber Security R&D Center includes a joint U.S.-Canada secure wireless trial, which tests the effectiveness of cross-border secure wireless architecture to cope with real time communication in a variety of scenarios. It also features the Linking the Oil and Gas Industry to Improve Cyber Security (LOGIIC) Partnership, an oil and gas sector model for public/private technology integration and demonstration to reduce vulnerabilities of process control environments.

The DHS Cyber Security R&D Center is also focused on improving next generation cyber security technologies. To accomplish this goal, HSARPA issues BAAs to: (1) improve the security of existing deployed technologies; (2) ensure the security of new emerging systems; (3) develop new and enhanced technologies for detection, prevention, and response to cyber attacks; and (4) facilitate the transfer of these technologies into the national infrastructure. These solicitations focus on specific technical topic areas, including system security engineering, operation security systems, and investigative and prevention technologies. They address all stages of R&D execution—applied research, development, and deployment.

The Center also manages other programs to address critical cyber security R&D topics. Over the past few years, the SBIR and RTAP Programs have addressed topics such as Botnet detection, exercise scenario modeling, real-time malicious code identification, and cross-domain attack correlation technologies. In addition, the Institute for Information Infrastructure Protection, a consortium of 30 academic and non-profit research organizations, has two major research programs that address process control and SCADA systems and economic and policy studies that examine return on investment. The Center's emerging threats thrust examines the virtual machine vulnerabilities and protection mechanisms, next generation crimeware defenses, and Botnet command and control detection and mitigation. The DHS–SRI International Identity Theft Technology Council brings together a group of experts and leaders from academia, Government, and the financial and IT sectors, and venture capitalists organized into four working groups addressing: (1) reports and studies; (2) data collection and sharing; (3) future threats; and (4) development and deployment. Finally, the Center's commercial outreach strategy assists companies in providing technology to DHS and other Government agencies and to enhance technology transfer from DHS S&T initiatives to larger security technology companies.

In summary, Dr. Maughan emphasized the Cyber Security R&D Center's aggressive agenda that is executed in close coordination with other Federal agencies and industry partners to strengthen technology diffusion and transfer and to identify migration paths to a more secure infrastructure. He noted the critical importance of public/private partnerships in maximizing the benefit of limited funds to solve the cyber security problems of current infrastructure and address future issues that will impact the Nation.

2.7 The Federal Plan for Cyber Security and Information Assurance R&D—Dr. Annabelle Lee and Dr. Simon Szykman

Mr. Copeland introduced Dr. Annabelle Lee, Director, Cyber Security Standards and Best Practices, NCSD, DHS, and Dr. Simon Szykman, Director, NCO/NITRD. Dr. Szykman provided an overview of the NITRD Program, which was established over 15 years ago and has its legislative basis in the *High-Performance Computing Act of 1991* and *Next Generation Internet Research Act of 1998*. The NITRD Subcommittee reports directly to the Office of Science and Technology Policy (OSTP) and has representatives from 14 program agencies as well as the Office of Management and Budget, OSTP, and NCO/NITRD. The NITRD Program represents the breadth of IT R&D portfolios across the U.S. Federal Government and is made up of eight program areas. Dr. Szykman noted that DHS joined the NITRD Program last year. The NCO supports NITRD-related policy making in OSTP and serves as the focal point within the U.S. Government for interagency technical and budget planning.

Dr. Szykman described the organizational structure of the NITRD Program and its program component areas. He noted that the NCO supports the President's Council of Advisors on Science and Technology, which is serving as the President's Information Technology Advisory Committee (PITAC). The Cyber Security and Information Assurance (CSIA) component area is a new addition to the NITRD Program, which aims to protect computer-based systems from action that compromises the authentication, availability, integrity, or confidentiality of these systems and the information they contain. The CSIA Interagency Working Group includes the formal members of the NITRD Program in addition to other participating agencies, such as the Department of Justice, Department of Energy, and Central Intelligence Agency. The working group, co-chaired by representatives from OSTP and a Federal agency, meets monthly to support interagency budget and program planning.

The CSIA Interagency Working Group developed the *Federal Plan for Cyber Security and Information Assurance Research and Development.* The plan serves as the basis for future roadmapping activities and future R&D policy, technical, and investment decision making. It identifies strategic Federal R&D objectives and a broad set of areas within the context of CSIA R&D. It highlights technical and investment priorities among these areas and makes broad findings and recommendations. The strategic objectives outlined in the plan are intended to guide the prioritization and evaluation of ongoing CSIA R&D initiatives. The plan is organized into eight technical categories: (1) functional cyber security; (2) securing the infrastructure; (3) domain-specific security; (4) cyber security characterization and assessment; (5) foundations of cyber security; (6) enabling technologies; (7) advanced and next generation systems and architecture; and (7) social dimensions. The top interagency funding and technical priorities are intended to inform and guide decision making, but are not a mandate for action. Dr. Szykman acknowledged that all 50 topic areas are important and noted that interagency priorities may differ from individual agencies' priorities. He also stated that the priorities identified in the plan are largely consistent with the critical R&D areas identified by the Information Security Research Council's Hard Problems List and the PITAC's Report to the President, *Cyber Security: A Crisis of Prioritization*.

Dr. Lee described the plan's high-level recommendations and findings: (1) target Federal R&D investment to strategic needs; (2) focus on threats with the greatest potential impact; (3) make

CSIA R&D an individual agency and interagency budget priority; (4) support sustained interagency coordination and collaboration; (5) build security in from the beginning; (6) assess security implications of emerging information technologies; (7) develop a roadmap for Federal CSIA R&D in conjunction with industry and academia; (8) develop and apply new metrics to assess progress; (9) institute more effective coordination with the private sector; and (10) strengthen R&D partnerships, including those with international partners.

In closing, Dr. Lee reviewed future steps. The NCO/NITRD is organizing workshops to validate information published in the Federal Plan for CSIA R&D with the private sector and academia and gather input from the non-Government research community to examine current initiatives, additional data, and potential gaps. The goal is to establish a framework for the CSIA R&D Roadmap.

3.0 LUNCHEON ADDRESSES

3.1 Luncheon Address—Mr. Michael Zafirovski

Dr. Peter Fonash, Deputy Manager, National Communications System (NCS), welcomed participants to the 2006 RDX Workshop and introduced Mr. Michael Zafirovski, CEO, Nortel. Dr. Fonash highlighted the importance of emergency preparedness in light of recent events, such as Hurricane Katrina. He commended Mr. Zafirovski for his focus on the identification of solutions to meet these outstanding challenges.

Mr. Zafirovski began his remarks by thanking Dr. Fonash and recognizing all participants for their involvement in the 2006 RDX Workshop. He described the importance of the NSTAC, noting its long tradition of bringing together leaders in the community to focus on the current challenges facing the telecom community everyone. He also highlighted the significance of holding this year's event internationally as all nations need to face these mutual challenges from a global perspective.

Shifting his focus to the converged NGN view, Mr. Zafirovski described the ability to make worldwide communications instantaneous. He noted the concern of senior leaders—if an event occurred near the U.S./Canada border, there is a fear that emergency response personnel from both countries would have difficulties communicating. He described a recent study of Wireless Fidelity (Wi-Fi) networks in London, England; Frankfurt, Germany; New York City, New York; and San Francisco, California. During this study, it was determined that more than 33 percent of the participating companies used unsecured Wi-Fi networks. Mr. Zafirovski noted that the health of international businesses are dependent on the need to secure threats to global cyber networks.

Mr. Zafirovski continued by describing Nortel's perspectives on cyber security. He specifically noted that Nortel recently made Lean Six Sigma a key part of its business plans to ensure improvement in robustness and quality for customers. He also highlighted a key principle for Nortel's product decisions, which focuses on the idea that there are no security-agnostic entities. Every technology, every piece of hardware or software, either augments or weakens the security of the overall network. As the demands for global security increase, Mr. Zafirovski cited the importance of several efforts to bring about alignment and interoperability in the emerging telecommunications technology areas. The T1.276 standard was published through the Alliance for Telecommunications Industry Solutions and adopted by the International Telecommunication Union and European Telecommunications Standards Institute (ETSI). Mr. Zafirovski stated that the T1.276 standard has expanded current Worldwide Interoperability for Microwave Access (WiMAX) capabilities to ensure secure applications across networks. He also highlighted the need for global-scale identity management as credentials for first responders increases into unmanageable numbers. He cited the importance of the conclusions for all topics at the 2006 RDX Workshop.

Mr. Zafirovski focused on key findings from customer perspectives. First, mobility and convergence are driving the NGN; however, serious concerns continue to mount over the availability of bandwidth for the NGN amid the increased interest in services that rely on this

bandwidth, such as mobile video and emergency responder reliance on WiMAX networks. Additionally, ad hoc ground communications will soon evolve into the need for a Fourth Generation network to address security responses and defense communications.

Secondly, Mr. Zafirovski noted the importance of network convergence as a driver of change in the communications environment. As businesses move their key information structures to data centers, business productivity will increase tremendously. Mr. Zafirovski continued to describe the increase in the reliance on secure cyber networks, highlighting cyber security concerns within the community. Finally, he outlined the future of the network to include an increased emphasis on communications devices and increased volume of traffic flowing over backhaul networks.

Mr. Zafirovski also noted the multimedia focus on 21st century Governments and enterprises. Based on the increased need for wireless and wired multimedia equipment, these entities expect airtight identity management and security within all networks. Mr. Zafirovski remarked on the changing needs and next generation of the industry's SCADA systems. He further noted the emergence of SCADA systems in today's critical infrastructures, whose networks are often relied on to support such things as chemical, biological, radiological, and nuclear sensors to monitor shipyards and nuclear facilities. Mr. Zafirovski highlighted the threat of this independent system to the economy.

Finally, Mr. Zafirovski addressed the services and solutions business, focusing on the complex nature of network convergence and the increasing demand for services. Based on this changing environment, Mr. Zafirovski highlighted the need for the communications industry to focus on network security to allow customers to focus on their businesses.

Mr. Zafirovski concluded his remarks by describing the reality that NGN trends are developing quickly and will continue to accelerate and he stressed the importance of the Government's role to develop policy supporting these changing trends. Mr. Zafirovski also commended the NSTAC and 2006 RDX participants for recognizing and fulfilling the need for coordination and collaboration.

(Note: the full text of Mr. Zafirovski's luncheon address is attached in Appendix C)

3.2 Luncheon Address—Dr. Veena Rawat

Dr. Fonash introduced Dr. Veena Rawat, President, CRC Canada, an agency of Industry Canada responsible for conducting applied R&D in communications and related technologies.

Dr. Rawat thanked organizers for holding the Workshop in Ottawa, Ontario, Canada and expressed her pleasure in participating in the event. She introduced the CRC's network security and public safety efforts by describing the Shirleys Bay Campus, a secure research facility where 400 CRC employees and 600 other researchers conduct cutting edge R&D. She explained that the CRC is part of Industry Canada, a ministry of the Federal Government. Dr. Rawat compared CRC to a conglomeration of missions of the National Telecommunications and Information Administration, NIST, and DOD. She noted that its mission is to be the Federal Government's Centre of Excellence for communications R&D, ensuring an independent source of advice for public policy purposes.

Dr. Rawat described CRC's core competencies—wireless systems, communication networks, radio fundamentals, interactive multimedia (such as broadcasting technologies), and photonics. The core competencies are organized into six major strategic priorities: (1) radio spectrum; (2) broadband; (3) applications; (4) defence communications; (5) network security and public safety; and (6) Internet/convergence policy. The Centre works to research, develop, and promote adoption of information and communication technologies and grow expertise.

Dr. Rawat provided an overview of CRC's organizational structure, noting that it is broken into four research branches, each with critical linkages to members of the S&T community. She emphasized the importance of information exchange among the branches— terrestrial wireless, satellite communication and radio propagation, broadcast technology, and broadband network technologies—and their industry and Government partners, international organizations, and academia.

Dr. Rawat described a few of the S&T projects CRC conducts on behalf of Government departments such as DRDC and Public Safety and Emergency Preparedness Canada. For instance, CRC improves radio communication interoperability by managing research, development, testing, evaluation, and deployment activities. Dr. Rawat also referred to the Spectrum Explorer as an example of CRC's technology development work. She mentioned software defined radio as well, a public safety application that demonstrates great technology transfer potential. Dr. Rawat also highlighted two additional public safety technologies—remote emergency management via satellite and broadcast and emergency warning systems.

Next, Dr. Rawat provided an overview of CRC's Network Security R&D Program. She emphasized this program's forward looking perspective and noted that it is focused on addressing the rising complexities associated with future systems and advanced techniques to detect and mitigate future attacks. Dr. Rawat described several prototypes aimed at detection, identification, and monitoring of malicious activities. She also mentioned policy based network management systems focused on enabling trust among peer organizations. Dr. Rawat reported that CRC is establishing a wireless security lab to expand the organization's security dimension through examination, testing and development of programs and products for Wi-Fi security, mobility, secure voice over Internet protocol (VoIP), ad-hoc network protection, and wireless transmission among others.

In closing, Dr. Rawat related both the breadth of CRC's activities and its in-depth focus on specific strategic areas. She also noted that CRC supports standards and prototype development, spectrum management, and test and evaluation through its R&D activities. CRC also contributes to commercialization by providing access to incubation facilities and testbeds.

4.0 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 as listed.

Breakout Session	Facilitators/Staff
International Internet Governance	Dr. Seymour Goodman, Georgia Institute of Technology Mr. Rod Wallace, Nortel Ms. Liz Hart, Booz Allen
Global-Scale Identity Management	Mr. Reg Foulkes, CSC Canada Dr. Tim Moses, Entrust Mr. Thad Odderstol, NCS Ms. Gretchen Sund, Booz Allen
Collaborative Mechanisms for Network Security Protocol R&D	Mr. Jim Brookes, Mathematics of Information Technology and Complex Systems Mr. Marc Sachs, SRI International Ms. Erin Comer, Booz Allen Mr. Charles Lancaster, NCS
Cross-Border and Cross-Sector Challenges	Mr. Stuart Brindley Dr. Jack Oslund Ms. Shelly Davis, Booz Allen
Wireless and Mobile Ad Hoc Network Applications	Mr. Mike Alagna, Motorola Dr. Julie Lefebvre, DRDC Ottawa Mr. Perry Fergus, Booz Allen Mr. William Fuller, NCS

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 and future R&D investment. To facilitate the discussion of international collaboration on cyber security R&D, participants were asked to consider the following questions:

- Various cyber security R&D initiatives are underway that aim to advance the security of free nations and enhance preparedness and response. Which aspects specifically require international coordination?

- What is currently being done to address this topic and how can it be leveraged to improve communications and increase the security and resiliency of the Internet?

- What technology areas offer the most potential to improve R&D in the future? Which area(s) should receive the most attention?

- 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 international collaboration for cyber security R&D 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.

4.1 International Internet Governance

Participants focused on the need for concerted R&D initiatives that address the challenges of international governance of preparedness and recovery efforts for cyber incidents involving the next generation of technology. Although participants acknowledged that technology is one way to secure the Internet, they also emphasized that governance, including policies and organizational mechanisms, are essential to better support cyber incident preparedness and response efforts. Such governance would not only foster an environment of trust in the networks, but would enable both international information sharing and coordination during incident response and information collection regarding Internet misuse.

4.1.1 The Current Landscape:

When considering the governance steps needed for cooperative international cyber incident preparedness and response, the participants identified several illustrative examples of the necessary components of cyber security and identified existing ("baseline") mechanisms that fulfill these requirements. The participants broke down the remaining discussion into three overarching areas subject to international governance: (1) infrastructure trust; (2) misuse and fairness; and (3) enforcement and resolution.

- **Infrastructure Trust:** Participants noted that in the current environment, users overall seem to have little trust in the security of the network infrastructure. The group noted that much of this mistrust is rooted in a lack of confidence by users in the management of route security, the existing Domain Name System structure, the E164 Number Mapping (ENUM) protocol, public web services, and party and device authentication capabilities. Such mistrust is only augmented by the global nature of the next generation of information and communication technologies (ICT)[1] networks. Today, the Internet is truly worldwide, with a presence in over 200 countries. In addition, cellular telephony is rapidly expanding across the globe. In fact, many estimate an additional 1 billion users will be added to the global Internet once

141

[1] While Homeland Security Presidential Directive 7 split the ICT sector into separate communications and information technology sectors for national security and emergency preparedness purposes, this distinction is not generally made throughout United States (U.S.) industry and internationally. As such, the sectors were discussed together as the ICT sector during much of the R&D Exchange Workshop.

VoIP brings the Internet into wireless phones. With increased users from around the world, the risk of attack and/or unsecure communications over the Internet will be even greater. International governance mechanisms will be necessary to monitor and regulate the use of the Internet to help thwart increased mistrust.

The participants considered the current "baseline" of governance mechanisms to foster infrastructure trust. They noted that current mechanisms, such as the U.S. Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* help to ensure secure access to U.S. Federal information systems. On an international level, the participants pointed to the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for the global coordination of the Internet's system of unique identifiers, such as domain names and addresses used in a variety of Internet protocols.

- **Misuse and Fairness:** Participants considered Internet misuse and fairness in the context of activities on the Internet that undermine trust in the security of the infrastructure. The group initially discussed the relevance of misuse from a content perspective, focusing on unsolicited commercial email, also known as SPAM. However, the participants agreed that for the purposes of the discussions, misuse should be considered from the perspective of activities that effect the architecture of the network, excluding application level abuses such as phishing. Examples of such misuse in the current operating environment include SPAM (as denial of service), mal-code that abuses the infrastructure, directed misuse of the infrastructure by adversaries, protocol misuse (Botnet), and abuse of Web services. Participants agreed that this type of misuse is not only undermining the public's trust in the Internet, but is also detrimental to the reliability and stability of the infrastructure. Since this type of misuse can originate from any location worldwide, there is a need for enforcement in an international governance model.

  Participants discussed current governance mechanisms that address Internet misuse. Among those mentioned were the National Cyber Response Coordination Group, established as a U.S. forum to coordinate intra-Governmental and public/private preparedness operations to respond to and recover from large-scale cyber attacks; the DHS Internet Disruption Working Group to address the resiliency and recovery of Internet functions in the event of a major cyber incident; the U.S. National Vulnerability Database, which serves as a comprehensive cyber security vulnerability database integrating all publicly-available U.S. Government vulnerability resources and provides references to industry resources; the Common Vulnerabilities and Exposures and the Open Vulnerability Assessment Language protocols; and some existing law enforcement mechanisms.

- **Enforcement and Resolution:** Participants agreed that to enable and foster a global culture of cyber security, international collaboration is needed for both real-time information sharing and coordination during incident response activities and information collection about Internet misuse and fairness. In considering such enforcement and resolution mechanisms, the globalspan of the Internet and private ownership of the infrastructure pose challenges. There are questions regarding the jurisdiction of cyber crimes, including elements such as the location of the parties involved and the location of the equipment. In addition, with the majority of the Internet infrastructure residing with the private sector, Internet governance

will need to balance the economic interests of industry and the national interests of Government.

With regard to current international governance related to enforcement and resolution of cyber crimes, the participants cited the Council of Europe Convention on Cybercrime Treaty, which received U.S. Senate ratification in August 2006. However, it was noted that the treaty does not provide a mechanism for the enforcement of the laws against cyber crime.

4.1.2 Challenges and Impediments

The group agreed on key challenges and impediments to international Internet governance that should be prioritized moving forward. Specifically, the participants noted areas requiring an additional "gap analysis" in each of the three overarching subjects.

- **Infrastructure Trust:** Although there are already some governance mechanisms, such as FIPS 201 for the U.S. Federal Government secure network access controls and ICANN for the safety and security of the global Internet naming system, without a further inventory and evaluation of current oversight processes and recommendations, there seems to be a lack of known international federation standards and legitimacy and mandate of current oversight. Recognizing the criticality of governance mechanisms in building user trust, the participants agreed that research attention needs to be directed toward understanding the international mechanisms that currently exist to protect the security of the infrastructure and the impact and effectiveness of these mechanisms. Specifically, a third party analysis of the current international oversight processes should be undertaken by subject matter experts.

- **Misuse and Fairness:** Second, the participants addressed challenges of misuse and fairness. The participants noted that although there are currently several mechanisms that address responses to misuse of the Internet, there are currently no prevention and mitigation mechanisms. Specifically, there needs to be a common understanding of what constitutes acceptable use of the Internet. Then, research should be directed toward mitigation mechanisms and should include stakeholder involvement from other critical infrastructures that might be impacted by an abuse of cyber infrastructure. In addition, research should consider incentives to discourage misuse of the Internet and liabilities for misuse. Specifically, there is a need to develop a common framework for information management and common assessment and mitigation tools.

- **Enforcement and Resolution:** There is no existing international cyber crime enforcement body or common enforcement framework. In addition, there is no multilateral mechanism to develop and implement criteria for horizontal coordination of cyber crime enforcement. It was suggested that R&D efforts should focus on verifying that no such mechanisms currently exist and then developing criteria and processes to achieve multilateral incident sharing and response.

4.1.3 The Path Forward

Based on the discussions, participants noted that future policy areas for NSTAC consideration should be given to: (1) multi-lateralization of the national security component of network security policy while maintaining the integrity of network operations; and (2) maintenance of the balance in governance mechanisms between national interests (of/or articulated by Governments) and economic interests (of/or articulated by business) in operation and stewardship of critical ICT infrastructure. In addition, participants identified three areas of future R&D:

- **Conduct an assessment and develop a catalogue.** Participants noted that there is currently no comprehensive understanding of existing international mechanisms for preventing and responding to international cyber incidents. Participants therefore agreed that research, through a third party analysis, should be conducted to develop an inventory and analysis of: (1) existing rules, relationships, and analogues from other sectors regarding network security policy and governance mechanisms; (2) the current "baseline" of national governance mechanism/policies in effect today for close allies; and (3) current components that should come under governance mechanisms as networks evolve to the next generation networks.

- **Develop structure and membership of multilateral governance mechanisms.** Participants suggested that once the above recommended research has been completed, development efforts should focus on determining the necessary structure and membership of multilateral governance mechanisms. These governance mechanism will achieve multi-lateralization of the national security component of network security while maintaining the integrity of network operations and the balance in governance mechanisms between national and economic interests in the operation and stewardship of critical ICT infrastructure. Specifically, with regard to membership, Participants recognized that, at this time, it may be more feasible to work closely with selected nations than to attempt to develop comprehensive, global governance mechanisms.

- **Investigate national and economic security implications of technical and economic convergence.** Participants recognized that policy and governance mechanisms aimed to maintain the balance of national and economic interests, will also need to be based on consideration of the national and economic security implications of convergence. Therefore, research in this area should be conducted to better inform policy makers.

The following table (Figure 1) clarifies the agenda for action discussed during the International Internet Governance breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

Figure 1. International Internet Governance Agenda for Action

Research Area	Recommended Focus
Conduct an assessment and develop a catalogue	• Existing rules, relationship, and analogues regarding network security policy and governance mechanisms • "Baseline" of national governance mechanism/policies • Current components that should come under governance mechanisms as networks evolve to the next generation networks
Develop structure and membership of multilateral governance mechanisms	• Multi-lateralization of the national security component of network security while maintaining network integrity • Maintenance of the balance between national security and economic interests of ICT infrastructure
Investigate national security and economic security implications of technical and economic convergence	• Conduct research to better inform policy makers

4.2 Global-Scale Identity Management

Participants distinguished identity management as a basic foundation for security on current and future cyber networks. They discussed various aspects of this multifaceted topic including authentication, access control, credentialing, privacy, trust, and usability, among others. The breakout session group identified challenges related to policy, processes, and human factors that outweighed perceived technical issues. Participants emphasized the need to develop scenarios and define requirements for a global-scale identity management solution. They agreed it would be important to examine how identities, attributes, and personas are managed in commercial systems that underpin critical infrastructure as well as Government systems with NS/EP applications. The group also recognized the need for interoperability amongst systems, agreement on terms, cross-recognition of practices, and development of business cases to accelerate global-scale deployment.

4.2.1 The Current Landscape

Discussion in the Global-Scale Identity Management breakout session focused on the need for agreement on attributes, conventions, policies, processes, schemas, standards, structures, and taxonomies for establishing and managing identity. Participants expressed a wide range of views on what constitutes an identity, which attributes are most important, and how multiple personas are best managed, authenticated, and assured.

Various bodies across academia, industry, and Government have repeatedly acknowledged the importance of embedding ubiquitous, interoperable identity management and authentication systems into future networks to ensure improved security within a dynamic threat environment. The NSTAC's *2004 RDX Workshop Proceedings* include a recommendation for additional research focused on usable, multilayered identity management and credentialing technologies and methodologies that provide end-to-end authentication of users and devices in the NGN. This

year, participants agreed that although a great deal of research and standards work is ongoing, none of the identified initiatives and activities fully address the requirements for the global-scale identification and authentication of people, applications, and devices accessing critical and sensitive information systems in the evolving network environment.

The group cataloged ongoing identity management activities and initiatives, including but not limited to the European Community's Daidalos Project, industry's IdenTrust system for digital transactions, and the U.S. Government's FIPS 201 initiative. They noted that most of the current work addresses commercial applications and does not focus on specific NS/EP requirements. Thus, participants agreed that it would be important to leverage existing initiatives and draw on the expertise in other forums. Participants identified five broad areas shaping the current landscape:

- **Ownership:** Participants discussed how an identity is constituted and what minimum set of attributes can be used to establish a unique identity. They raised questions regarding cross-recognition and sovereignty. Specifically, participants articulated the need for a common framework to create consensus on how identity information is used to build trust in an individual, device, or application and grant access, credentials, and privileges.

- **Assurance, Risk, and Trust:** Participants indicated that in the global network environment there is a high premium for a usable, trusted system that creates a reasonable level of assurance that a person or object is who or what it purports to be. Participants focused on the need for models that would guarantee graduated levels of assurance and reliability, according to perceived risks. They recognized that there will be failures; therefore, systems should be augmented with multiple security techniques (for example, real-time intrusion detection systems) to improve their integrity and trustworthiness.

- **Privacy:** Participants held divergent views on the trade-off between privacy and convenience. Some believe that the advent of new identity management technologies requires vigilant protection of personally identifiable information that is susceptible to theft, compromise, and loss. Others were willing to voluntarily give up personal data to achieve greater efficiencies. Privacy safeguards must be balanced with legitimate national security needs.

- **Market Influences:** Participants recognized the distinct difference between consumer and NS/EP applications and the need for business incentives to accelerate global-scale deployment of identity management systems. Participants underscored the importance of commercial drivers such as competitiveness, trade implications, and regulatory mandates but acknowledged that market forces alone will not produce acceptable levels of security and assurance for NS/EP use.

- **Global Cooperation & Adaptability:** Participants agreed that it is unlikely that a single identity management solution will take root globally; thus, the development of separate but compatible systems is more practical. However, this outcome relies on cross-recognition of certification practices, credentials, data schema, and protocols. Participants also acknowledged the need for solutions designed to accommodate continual security upgrades and to function with the various technology generations present in the network.

4.2.2 Impediments and Challenges

The breakout session group identified four major impediments to the development of global-scale identity management solutions:

- **Components of Identity:** Progress will be very difficult without agreement on the components of identity. Without a common understanding of the minimum set of attributes that constitute an identity, the development and adoption of universally compatible systems is unlikely. Therefore, it is imperative to gain widespread agreement on the requirements and properties of identity.

- **Individual Identity Management Systems:** Sovereign nations are bound to develop their own identity management systems. The current environment, characterized by a universe of activity and limited global coordination, reveals the political impediments that create barriers to the establishment of a single, universal identity management solution. User acceptance of deployed systems is also an important consideration. For widespread adoption to be possible, solutions must be implementable, interoperable, affordable, scaleable, and easy to use. Enabling global acceptance of trust is another critical challenge. When individuals, organizations, objects, and processes have multiple sources of authenticated identifiers, various personas, and diverse platforms, it is difficult to achieve consensus and compatibility.

- **Adoption of Global-Scale Systems:** In addition, there is a lack of motivation to adopt global-scale systems in the current environment. Incentives, such as tax breaks, and/or drivers, such as regulatory mandates, must be put into place to spur action. The time and cost associated with infrastructure development has discouraged widespread adoption of a broadly applicable solution. International dialogue about the division of roles and responsibilities and allocation of resources is needed to enable global-scale identity management systems that meet NS/EP requirements.

- **Privacy and Civil Liberties.** Concerns about protecting privacy and civil liberties impede adoption of solutions globally. Many users resist revealing personal information due to a fear that it will not be sufficiently protected. To entice voluntary, cooperative participation the value proposition must deliver a strong benefit in the point of view of a large and diverse user population.

4.2.3 The Path Forward

As a result of the discussion, participants identified next steps necessary to advance global-scale identity management and meet NS/EP requirements on the NGN:

- **Identify Centers of Excellence for identity management R&D to encourage collaboration, maintain a repository of ongoing initiatives, and identify promising technologies.** To promote education and awareness and strengthen the research community's capability to collectively capitalize on advancements, participants emphasized the importance of creating a better understanding of the universe of current initiatives. They recommended pinpointing international Centers of Excellence focused on identity management and supporting cooperation. Participants also agreed that a catalog of existing

activities would help to educate researchers, improve awareness, and enable mutually beneficial collaborative relationships.

- **Develop cross-border and cross-sector use-case scenarios and requirements.** Participants determined that R&D for global-scale identity management solutions could not be justified without a better understanding of scenarios and requirements. Although participants agreed that identity management is critical for NS/EP services, such as information sharing and priority access, they recommended that scenarios be developed to determine requirements and improve the business case for the development of global-scale systems.

- **Define ownership of identity.** Given the increasing number of communicating users, processes, and devices, identity will be required more frequently, in a broader number and type of settings, on the NGN. As demand for authenticating and authorizing users increases, it will become even more important to understand who owns the information collected and how it will be protected, used, stored, accessed, and transferred across domains. The fundamental question of ownership will substantially influence how identity is managed in future networks.

- **Advocate for agreement on models for assurance, risk and trust.** Common frameworks for assurance, risk, and trust are critical to enable the development of interoperable, broadly applicable identity management solutions. In the NS/EP environment, careful consideration of assurance levels, risk management practices, and trust mechanisms are critical to accelerating security and reliability on the NGN. Participants acknowledged the need for dialogue and agreement around graduated levels of assurance, risk appetite, and inter-domain trust.

- **Create a common taxonomy to improve communication and collaboration.** Participants discussed the need to develop a glossary of terms to create mutual understanding and to enable cross-border and cross-sector collaboration. A common vocabulary allows a large and diverse population of users and practitioners to communicate and cooperate. Given the need for interoperability and compatibility, a shared vocabulary is essential to identify requirements, and harmonize efforts. Without a common taxonomy, a cohesive effort to ensure that NS/EP requirements are understood, embedded and addressed in future identity management systems is impossible.

- **Adapt privacy policies and resolve legal and liability issues.** Participants agreed that legal and liability issues could impair the adoption of a federated, interoperable identity management framework. They also noted that identity management systems would need to include explicit protections for privacy. Careful consideration of individual rights and legal and regulatory issues is necessary for widespread adoption and acceptance.

- **Advance supporting and interoperable infrastructure.** Identity management systems require underlying infrastructure that can be both expensive and time-consuming to build. However, compatible, interoperable solutions require a substantial investment in infrastructure. Expenditures must be justified through value propositions that consider incremental benefits and clearly articulate returns.

The following table (Figure 2) clarifies the agenda for action discussed during the Global Scale Identity Management breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

Figure 2. Global Scale Identity Management Agenda for Action

Research Area	Recommended Focus
Identify Centers of Excellence for identity management R&D	• Support cooperation in identity management • Catalog existing activities to educate researchers improve awareness, and enable mutually beneficial collaborative relationships
Develop cross-border and cross-sector use – case scenarios and requirements	• Development of scenarios to determine requirements and improve the business case for the development of global-scale systems
Define ownership of identity	• Clarity of information ownership to alleviate later complications • Assurance that information will be protected, used stored, accessed, and transferred across domains in accordance with accepted privacy principles
Advocate for agreement on models for assurance, risk, and trust	• Careful consideration of assurance levels, risk management practices, and trust mechanisms to accelerate security and reliability on the NGN • Greater emphasis for dialogue and agreement around graduated levels of assurance, risk appetite, and inter-domain trust
Create a common taxonomy to improve communication and collaboration	• Development of a glossary of terms for users and practitioners to communicate and cooperate, identify requirements, and harmonize efforts
Adapt privacy policies and resolve legal liability issues	• Requires explicit protections for privacy • Requires consideration of individual rights and legal and regulatory issues
Advance supporting and interoperable infrastructure	• Requires substantial investment in infrastructure • Justification of expenditures through value propositions; cost-benefit analysis

4.3 Collaborative Mechanisms for Network Security Protocol R&D

Participants immediately recognized the importance of developing international collaborative mechanisms to foster greater global network security protocol R&D. They acknowledged that currently no such mechanism exists; but conceded that the global phenomenon of interconnectivity via the expansion of the telecommunications network and the Internet in combination with growing national and homeland security threats requires a new paradigm for ensuring network security. Participants agreed that a plethora of existing models and mechanisms could provide essential components in the development of an overarching framework to address their concerns. Upon deeper evaluation of the topic, participants agreed that the collaborative mechanisms discussed should not focus solely on network security protocols but network security in general, and they agreed to base their further discussion on this broader topic.

Participants commenced their discussion on collaborative mechanisms by reviewing past RDX Workshop investigations on the subject matter and discussing the value of using the Semiconductor Manufacturing Technology (SEMATECH) Partnership as a baseline model for developing a global partnership to address network security R&D. Past RDX Workshop participants noted that discussion at the 2003 and 2004 Research and Development Exchange Workshops recognized the critical need for increased collaboration between all stakeholders to ensure that NS/EP requirements are met on future networks. By combining the skills, resources, and assets of each sector, a collaborative partnership for network security R&D could deliver more effective products and services in a more affordable manner than could otherwise be achieved.

A participant briefly outlined the purpose of the SEMATECH Partnership which was developed as a solution to the coordinated commodity memory chip dumping in the U.S. market in the late 1980s and early 1990s from producers in Japan and other areas in Asia. The partnership took advantage of the *National Cooperative Research and Development Act of 1984* and was formed when semiconductor manufacturers and the Federal Government collaborated to fortify the U.S. semiconductor market by uniting to address manufacturing problems in 1987. The DOD appropriation of $500 million, with a matched investment by industry members, provided SEMATECH the necessary resources to create successful solutions that allowed the U.S. chip industry to reclaim its firm position in the market. Participants quickly agreed that while SEMATECH represents a successful model for managing the security risks associated specifically with the semiconductor community, the threats facing the global telecommunications network are far more broad and non-specific and thus require a different approach.

4.3.1 The Current Landscape

Participants noted that no overarching, worldwide network security partnership exists to address network security issues despite the diverse and quickly emerging global threats to the telecommunications infrastructure. They noted that efforts to address network security R&D are typically accomplished at the domestic level by industry and Government entities focused on national or corporate interests and are rarely even discussed amongst allied nations due to strict legislative and regulatory concerns. Participants further acknowledged that such a body is unlikely to be developed spontaneously within the private sector as many corporation view national security and public safety issues as falling within the Government domain on act primarily on issues driven my market forces.

Participants did note, however, that positive attributes of numerous existing models (see Figure 3) and mechanisms (see Figure 4) at the domestic level could be leveraged in the development of a global network security R&D partnership.

Figure 3. Collaborative Model Approaches

Collaborative Model Approaches	
• Grants • Membership • Cooperative Research and Development Agreement • Volunteer-based • Memorandum of Agreement	• Bi/Multilateral • Treaty • Economic Initiatives • Government-centric • Industry-centric

Figure 4. Current Collaborative Mechanisms

Current Collaborative Mechanisms	
• Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) • Cyber Defense Technology Experimental Research project • Planet Lab • Internet 2 • Carnegie Mellon University: Cylab • Cooperative Association for Internet Data Analysis • Canada's Network Centres of Excellence Program • The Technical Cooperation Panel • The European Commission's Framework Programme for Research and Technological Development	• Public Security Technology Program • BITS Financial Services Roundtable • National Science Foundation: Global Environment for Network Innovations • Research Triangle Park • LOGIC • Institute for Information Infrastructure Protection • DHS S&T: Technical Support Working Group • Central Intelligence Agency: In-Q-tel • Semiconductor Manufacturing Technology • Institute of Electrical and Electronics Engineers • Network Security Information Exchange (NSIE)

4.3.2 Challenges and Impediments

Participants identified numerous overarching impediments/challenges to international collaboration on network security issues.

- **Laws and Regulations:** First, participants raised the extensive and far reaching laws and regulations that impede industry from working together effectively in the U.S. These laws and regulations include, but are not limited to, intellectual property, copyright, and patent restrictions; export control laws; the International Trade and Arms Regulations; the *Freedom of Information Act*; anti-trust restrictions; and restrictive data markings placed on materials by the Federal Government. Efforts to work collaboratively at an international level must not only take into consideration U.S. laws and regulations, but similar restrictions in other countries also participating in the effort,. This can lead to the potential for an extremely

complex and burdensome participation approval process that could quickly stymie any intended collaboration.

- **Market-Driven R&D Issues:** Participants reflected on the failure of the international communications market to generate interest in collaboratively addressing compelling R&D issues. They noted that the marketplace relies on Governments to address public safety, economic viability, and social issues caused by threats to the Internet and its related technologies; therefore, it would not assume responsibility for establishing an international R&D body to address these Governmental functions on its own accord. The group further agreed that a variety of other factors including the fact that the private sector perceives that the market does not effectively address public infrastructure problems, uncertainty related to the risks the Nation faces, and the scope of the collaboration required all impact the desire and/or ability of the market to respond to NS/EP-related R&D. Consequently, they agreed that Governments must respond to the inefficiencies and gaps caused by market activity to address issues of the common good.

- **Perceived Benefit:** Members observed that the lack of a clear equation for determining benefit from the collaborative effort based on contribution could hinder participation. Participants recognized the inability of all participating entities to contribute similar personnel and financial resources to a collaborative effort and agreed that without a clear understanding of the resource commitment from each participating entity and the associated "tiered" benefit received, members may not wish to participate.

- **Protection of Member Data:** Participants concurred that protection of member data is essential for the effective functioning of the collaboration. Without the publication of clear data protection guidelines and the establishment of methods for enforcing these guidelines, participation will be hindered.

- **Member Commitment and Community Endorsement:** The group emphasized the essential nature of member commitment to and community endorsement of the collaborative effort. Without support from these two communities, the collaborative effort will be unable to sustain its activities over the long term and accomplish its goals.

- **Security Clearances:** The group also noted the negative effect that citizenship and security clearances for students might have on collaboration.

4.3.3 The Path Forward

In evaluating the next steps for internationally fostering enhanced network security collaboration, participants identified three critical activities that must be undertaken by the international telecommunications network security community:

- **Create an international R&D Consortium.** Participants noted that the Consortium must, to be effective, meet a variety of high level and discrete criteria. At the broadest level, the Consortium must enable collaboration on "big ticket" security research topics; be sustainable in the long term; address the compelling network security risks to public safety and economic sustainability; be guided by clear funding, technology transition, and intellectual property principles; offer 'Safe Harbor" protection from legislative and regulatory restrictions; and be

supported by member practices based on trust and openness. In addition, participants emphasized that the Consortium must support the networking and collaboration of all participants, provide advocacy for needed research, seek community endorsement, and provide meaningful output for participants.

- **Enlist an inspiring Champion to launch the international R&D Consortium.** As the primary driver of the Consortium, participants agreed that the Champion must take responsibility for establishing not only the entity's guiding framework but also facilitating the establishment of relationships between member participants. Specifically, the Champion should define the Consortium's business plan and develop its funding proposal; define and establish the international collaboration framework including its governance model; develop the value proposition for each group of participants; and engage international partners. Furthermore, the Champion should identify and communicate with those key stakeholder groups interested in contributing to and benefiting from the Consortium's expertise and products.

- **Establish a research agenda that identifies and works on the highest priority issues as raised by the Consortium's partners.** While the research agenda must ultimately be defined by the Consortium's partners and evolve with time, participants recommended that the Consortium include amongst its top priorities wide scale situational awareness for attack prediction and detection, more resilient and secure network protocols, global scale authentication and identity management, secure and scaleable routing infrastructures, and security metrics. Moreover, participants also highlighted a variety of additional topics for further investigation, including deployment of R&D solutions, the dynamic risk environment, a strongly authenticated network control plane, and improved and implemented software and system engineering methodologies. Participants strongly stressed the importance of ensuring commitment to support and implement agreed upon solutions once developed to benefit from the activities of the international R&D Consortium.

Recognizing the strong role that policy will play in facilitating the establishment and conduct of the international R&D Consortium, participants also recommended that the NSTAC, or an international counterpart, address a variety of associated issues, including:

- Legal concerns associated with sharing intellectual capital amongst member entities including anti-trust and freedom of information laws;

- Governmental policy for sharing information across borders;

- Privacy of individual citizens;

- Membership eligibility for an R&D Consortium; and

- Appropriate role for Governments in the R&D Consortium.

The following table (Figure 5) clarifies the agenda for action discussed during the Collaborative Mechanisms for Network Security R&D breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

Figure 5. Collaborative Mechanisms for Network Security R&D Agenda for Action

Research Area	Recommended Focus
Situational Awareness	• Creating wide scale situational awareness for attack prediction and detection
Protocols	• Developing more resilient and secure protocols
Global scale authentication and identity management	• Developing global scale authentication and identity management mechanisms
Routing Infrastructure	• Establishing a secure and scaleable routing infrastructure
Security metrics	• Development of security metrics

4.4 Cross-Border & Cross-Sector Challenges

Participants agreed that limited collaboration, including, but not limited to, R&D, has created a major impediment to the creation of successful cross-border and cross-sector initiatives supporting the telecommunications sector. They discussed how the sectors continue to remain stove-piped and localized despite the increasingly interdependent environment. Absence of trust relationships, sector-specific jargon, and proprietary issues are subjects still unaddressed by sector leaders. Participants emphasized the need for enhanced private cross-sector participation in government discussions, where appropriate, R&D categorization, interdependency modeling, and exercising as means to breaking down the barriers that inhibit international collaboration.

4.4.1 The Current Landscape

Unlike the other breakout sessions, this session's focus was broadened to include Critical Infrastructure Protection as well as cyber security. Participants began the breakout session by first describing the interconnectedness between the U.S. and Canada, which is emphasized by the interdependency between the electricity and telecommunications critical infrastructures. They continued their discussion on past cyber security policy and strategy initiatives in the U.S. including two specific strategies: (1) *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*; and (2) *The National Strategy to Secure Cyberspace*. Participants noted that initiatives must be coordinated across borders to ensure the success of either strategy. The facilitators encouraged breakout session participants to engage in "out of the box" thinking in addressing the basic interdependencies between the physical and cyber portions of the networks. The participants identified three major areas shaping the current landscape:

- **Identifying Interdependencies:** The facilitators described the interdependency between the electricity and telecommunications in further depth. They noted that while many critical infrastructure experts believe the electricity infrastructure is most important to all critical infrastructures, they recognize the electricity industry relies heavily on the telecommunications infrastructure to support their SCADA systems and restoration processes. Participants discussed an interdependency assessment conducted in Ontario, Canada, in 2002, and they agreed that the last mile of telecommunications connectivity remains most important to the user community. One participant emphasized the communications redundancy that has been established by the electricity sector: circuits run

across both virtual private networks and the public switched telecommunications network. Another participant noted that three types of communications in the electricity sector are necessary: (1) voice; (2) protective circuits; and (3) telemetry used to continuously monitor and control the electric grid.

- **Global Cooperation and Communication:** Participants recognized the differences in the technical languages associated with various critical infrastructure sectors. Participants agreed that communication coordination between the sectors is key to achieving solutions that can be used in cross-border and cross-sector situations, especially in response to globalization and the consequential increasing international scope of interconnection. Several group members highlighted the need to engage multiple countries, sectors, and user groups in defining a common language that can be used for all critical infrastructures.

  In addition, group members noted the lack of interest in engineering and technical degrees from the next generation of subject matter experts (SME). There was a growing concern within the group that college students are not interested in technical topics, which will decrease the SME employee pool in the near future. Participants also noted the changing environment in application use across the Internet. One participant cited MySpace.com and YouTube.com as examples of increased application use of the Internet by today's generation of users. Group members recognized the significance of these new Internet services and the increased security risks they pose. Participants also recognized that use of these services and the emergence of new services are expected to increase in the next few years.

- **Research and Development Initiatives:** Breakout session participants agreed that they should discuss suggested R&D initiatives for the telecommunications and electricity sectors. Participants noted that both infrastructures are similar in nature; therefore, they will likely face similar cyber challenges in the future. Group members stated that all sectors have similar R&D priorities; however, information on cyber security and information assurance priorities across industries does not exist.

  Participants also discussed the lack of information around current R&D initiatives supporting cross-border and cross-sector challenges. One participant suggested that R&D initiatives do exist; however, they are limited in scope and mainly mission-driven for a particular entity. They cited the lack of a database mechanism where information could be shared on interdependency initiatives. Another group member highlighted a collaborative approach currently in use in Europe. Details on this approach were discussed within the group, and they determined that is somewhat limited, based on the requirement for participation from at least two corporations, at least two European countries, and one academic institution. Participants identified a few R&D activities that are currently underway and suggested they be leveraged in support of future R&D initiatives, including:

  - **The Roadmap to Secure Control Systems in the Energy Sector.** The U.S. Department of Energy partnered with industry to create this roadmap, describing a framework for research initiatives focused on securing the energy control systems and describing the inherent dependence on the communications infrastructure.

- **The Technical Cooperation Panel.** This panel was developed by the five Allied nations as a mechanism to share information on research activities to minimize redundancy.

- **The LOGIIC Consortium.** DHS collaborated with industry members to form this consortium to help protect oil and gas operations from cyber security threats, such as viruses, worms, and cyber terrorism.

4.4.2 Impediments and Challenges

Participants identified four overarching impediments/challenges to Cross-Border & Cross-Sector collaboration:

- **Information Sharing:** Participants noted several human and social issues related to information sharing across sectors and borders, including that several critical infrastructure owners and operators concerns about international issues associated with information sharing. A participant highlighted the information sharing progress made in the past few years; however, participants concluded that legal agreements and safeguards are needed to further promote voluntary information sharing across borders. They highlighted that the agreements must also be socialized within the respective communities to increase awareness. Breakout session participants also noted the importance of relationships to achieve information sharing and recognized that relationship-building is focused on trust, which requires significant time to develop. Participants discussed current information sharing mechanisms, such as the Information Sharing and Analysis Centers (ISACs) and the Partnership for Critical Infrastructure Protection (PCIS) in the U.S. It was stated that these exchanges should also be used to share information and research priorities between industry and Government.

  Another impediment to cross-border and cross-sector information sharing is the limited willingness or ability to share classified or sensitive information. Participants agreed that several barriers exist to establishing new partnerships and broadening existing partnerships. One participant suggested that government leadership was needed to raise the profile and value of this collaboration with private sector leaders and to develop a plan for expanded bilateral and multilateral coordination. Another participant raised a concern over a tendency for government policymakers to favor new security products over the value of building industry/government partnerships. Group members also agreed that engaging the community in common goals and priorities would showcase the value of relationships.

- **Leadership:** Participants discussed the lack of coordinated leadership around developing risk-based approaches for prioritizing resources specific to cross-border and cross-sector issues. Group members expressed concerns over the tendency of government policymakers in managing resources and research priorities to overemphasize very low probability events. Additionally, participants noted that industry and Government often struggle with differing opinions on cost and schedules for R&D.

- **Cross-Sector Interdependencies:** Group members discussed the need to model and analyze cross-sector interdependencies. They recognized that it is critical to establish at the outset

the "ground truth" on interdependencies before any modeling is undertaken.. Participants agreed that the interdependencies presently are not understood well enough to achieve results from modeling and analysis efforts. One participant suggested that the Government should approach insurance companies to leverage their thoughts on risk models and interdependencies. While agreeing with the idea, participants cited concerns over the ability to leverage the insurance industry methodologies since the communications industry cannot define a final cost associated with loss or impact.

- **Spectrum Allocation:** In addition, participants discussed the competitive nature of spectrum allocation databases across borders. One participant stated that each country has a process for achieving spectrum resiliency; however, it is not bi-nationally coordinated. Participants agreed that current processes and opinions should be documented before cross-border arrangements can be discussed. One group member suggested examining the NSTAC's 1996 concept paper, *Information Security Standards Board,* as an example for this type of arrangement. Another participant questioned whether military standards for spectrum allocation and cross-border interoperability could be leveraged for first responders and the private sector. Group members agreed that current laws either impede or do not allow users to achieve interoperability, and that consideration should be given to allowing critical infrastructure owners and operators to have the same spectrum domain as the first responder community.

4.4.3 The Path Forward

Participants recognized the importance of agreeing to the top priorities for R&D in the areas of cross-border and cross-sector physical and cyber security. The following items were suggested as steps to improve the inter-industry and international challenges.

- **Define a plan for research on interdependencies.** Participants agreed that this plan should address the goals towards securing the interdependencies between and among sectors, including, but not limited to, the electricity and telecommunications sectors, and highlighted that the plan should focus goals on the NS/EP portion of securing the network. Participants recognized that while significant research activities are currently focused on cyber security, they do not exist in an NS/EP context.

- **Develop collaborative mechanisms to ensure secure SCADA systems.** Group members agreed that SCADA systems are becoming increasingly more important to the reliable operation of the electric grid; therefore, collaborative mechanisms must be implemented to ensure success across borders and among sectors.

- **Coordinate resilience exercises.** Participants recognized that coordinated planning and exercises exist to varying degrees across borders within each sector. However, interdependencies have not been exercised regularly by operations employees to test resilience. Participants agreed that conducting exercises regularly helps to build trusted operational relationships. .

- **Investigate a common spectrum database.** Participants recognized that spectrum databases exist in most countries; however, they are not shared. Participants cited the need to share information across borders and to develop a common database for spectrum allocation.

- **Develop a plan for expanded bilateral and multilateral coordination.** Participants highlighted the effectiveness of existing government bilateral agreements and agreed on the need to extend these relationships to include private cross-sector participation, as appropriate. Participants further suggested that multilateral agreements should also be built, based on common interests and goals, and should include industry participation, as appropriate.

The following table (Figure 6) clarifies the agenda for action discussed during the Cross Border and Cross Sector Collaboration breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

Figure 6. Cross Border and Cross Sector Collaboration Agenda for Action

Research Area	Recommended Focus
Define a plan for research on interdependencies	• Plans should focus goals on the NS/EP portion of securing the network (current focus is cyber security)
Develop collaborative mechanisms to ensure secure SCADA systems	• Prioritization of SCADA systems due to their increasing vulnerability • Implementation of collaborative mechanisms to ensure success across borders ad among sectors
Coordinate resilience exercises	• Carry out regular exercises to test the effectiveness and usability of established systems
Investigate a common spectrum database	• Utilization of the databases established in most countries to create a shared database for spectrum allocation
Develop a plan for multilateral coordination	• Extension of existing bilateral relationships to enhance private cross-sector participation (common interests and goals)

4.5 Wireless and Mobile Ad Hoc Network Applications

Participants emphasized the significant potential for wireless and mobile ad hoc network (MANET) technologies to deliver assured communications in support of an expanded range of users to include military, NS/EP, disaster response, and first responder communities of interest. To realize this potential, essential R&D focal points include addressing not only fundamental MANET technical and security shortfalls but also critical human factor, organizational, jurisdictional, and economic/business case considerations.

4.5.1 The Current Landscape

The participants identified six major areas shaping the current landscape with regard to wireless and MANET applications.

- **Communications Functionality:** Participants reviewed the promise of wireless network and MANET technology to deliver enhanced communications functionality, specifically in support of the emergency response community. Group members also affirmed that focused discussion of the topic as a part of the R&D Exchange was both apt and constructive. One member noted that an ad hoc networking approach may be particularly effective in situations where the underlying communications infrastructure has been destroyed or is otherwise unavailable, and members identified other operational benefits to include robust connectivity, ability to mitigate single points of failure, potential for increased capacity, inherent fault tolerance (self healing), and overall architectural design and implementation flexibility.

- **Security:** Participants identified security as a fundamental issue regarding barriers to potential wide scale adoption of wireless ad hoc network capabilities to support mission critical environments. Participants noted inherent differences between the current static network security environment and a notional future ad hoc environment in which dynamic MANET topology changes (characterized by rapid addition and deletion of network nodes/users) will have significant implications for how stable authentication, authorization, routing, and intrusion detection and protection are effectively realized.

- **Unique Communications Needs:** Participants discussed the application of wireless network and MANET technologies to meet the unique communications needs of national security, emergency response, and public safety communities. A member noted that the specific communications network security requirements will be largely dependent on the application. For example, in a life-and-death emergency response situation, communications system operability is the principal concern whereas security is likely tangential. Participants then identified three categories of scenarios with dissimilar levels of security requirements: (1) temporary MANET implementations in which operability is essential and security may not be as critical; (2) permanent implementations in which security is a critical and obligatory component of network design; and (3) "middle ground" implementations in which the level of security applied will vary based on user need. The participants reached a basic consensus that, regardless of category or application, security should be considered proactively in the network design phase and not reactively inserted after network deployment is complete.

- **Lessons Learned:** To further identify and debate potential wireless network and MANET benefits and shortfalls, participants shared some operational and technology trial experiences. Participants discussed lessons learned regarding restoration of communications capabilities during the Hurricane Katrina response effort and approaches to mitigate existing interoperability issues with land mobile radio (LMR) systems. Several members emphasized the criticality of ensuring both system operability and interoperability, cautioning against too much attention on the latter at the expense of the former.

- **Wireless Solutions:** Participants also described their experiences with deployable wireless solutions, including the switched-satellite access component of the communications system featured in the recent U.S.-Canada Secure Blackberry trial and a U.S. DOD-based deployable cellular communications solution. The group discussed these examples noting that both systems enable reuse of commercial cellular spectrum and feature automatic system shutdown upon recovery/restoration of the commercial cellular infrastructure. A participant described the Communications Asset Survey and Mapping capability, a database tool that

can support public safety LMR system interoperability planning through coordination and sharing of available interoperability frequencies. Another participant described the recent "Strong Angel" disaster response exercise in which frequency interference issues between wireless ad hoc networks were common due to lack of pre-coordination. Members agreed that establishment of a well-defined coordination policy, involving relevant industry, Government, and academic stakeholders is critical to resolve many of the issues identified in field testing and operational environments.

- **Current R&D Activities:** As a part of a brainstorming exercise, participants identified examples of current R&D activities that address wireless networks and MANETs and serve to enhance overall communications and cyber security. Participants identified and prioritized key technology areas that offer the most potential to improve MANET security and interoperability R&D in the future. The group also highlighted specific research focus areas within the academic community. Figure 7 lists selected R&D activities and key technology focus areas identified during session discussion.

Figure 7. Current R&D Activities and Key Technology Areas

Current MANET R & D	
• European Union: Wireless Deployable Network System Project • NIST: MANET & Sensor Network Security Project • NIST: Distributed Test Bed for First Responders • Telecommunications Industry Association (TIA) and ETSI: Project Mobility for Emergency and Safety Applications	• U.S. Army Communications-Electronics Research Development and Engineering Center: Multi-Dimensional, Assured, Robust Communications for On-the-move Network-I STO Program • Defense Advanced Research Projects Agency Projects • Defense R&D Canada Projects
MANET Key Technologies and Academic Areas of Focus	
• Global Deployments/Registry* • Group Key for interoperability, dynamic changes and scale* • Test Bed/Standards/Certification/Requirements* • Location-based Service* • Mobility/Usability Features, including authentication (biometric, voice), authorization, audit, Quality of Service (QoS) + Security (priority), intrusion detection and protection, denial of service protection, and hybrid networks* • 802.11 i/n Automated Security (and others) • Customized simple chip (low cost) ** Identified by members as high priority items*	• Sensors + Radio Frequency Identification • Cognitive radio/Software Defined Radio/Spectrum • Technology approaches to privacy issues • Policy-based management • Human Factors/Interface • Development and sharing of best practices • IP and IP version 6 • Identity-based encryption • Discovery mode strategies • Extension of traditional security approaches to MANET • Lightweight cryptography • Priority access/QoS

4.5.2 Challenges and Impediments

Participants identified three overarching impediments to increased wireless network and MANET acceptance and R&D.

- **"Killer Application" for MANET Technology:** Participants recognized that in the commercial application space, the so-called "killer application" for MANET technology does not yet exist. Participants noted both the emphasis of current MANET research on military applications and the lack of a mature and documented business case for MANET non-military uses. Related to this lack of business case justification for MANET use, participants noted that the current market environment also lacks an overarching MANET deployment vision or concept of operations that would specifically justify an augmented R&D focus and resource allocation.

- **International R&D Coordination:** Group members agreed that ongoing international R&D activities are not well coordinated, particularly from a bilateral or multilateral perspective. Participants agreed that increased cross-border coordination of ongoing R&D activities was warranted to better leverage available R&D resources.

- **Secure MANET Architecture Transition:** Participants identified and discussed a range of transition issues from the current environment to the notional ideal of a secure MANET architecture. Issues identified included human/culture factors and barriers, acceptance of multinational standards, the lack of suitable test-beds for security and accreditation, security clearance level and foreign disclosure constraints to greater information sharing, intellectual property rights and export control considerations, privacy and liability concerns, and an overall lack of community of interest forums to better socialize the need for MANET R&D.

In summarizing challenges and impediments to increased wireless network and MANET deployment and R&D, participants reached a general consensus that not enough was being done with regard to education and training, standards development and implementation, interoperability, reducing security costs, and development of testing cases that involve international collaboration.

4.5.3 The Path Forward

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

- **Identify and address human factor barriers to increased R&D to include cultural, governance, jurisdiction, and trust issues.** Participants noted that the primary barriers to increased MANET R&D are not necessarily technological in nature. Rather, the diverse range of private and public sector stakeholders must collectively address the significant organizational, jurisdictional, and basic trust enabling issues that continue to exist, particularly in an operational environment. Participants identified specific investment areas to include identity management for "global, dynamic, technology-agnostic, hierarchical, meshed networks;" use of technologies and capabilities that enable communities of interest; and full consideration of human factors in technology development, planning, and exercises.

- **Open doors to foster collaboration, innovation, information sharing, R&D sharing and coordination, and standards and policy development.** In keeping with a recurring theme voiced throughout the R&D Exchange, participants emphasized the need for collaborative mechanisms to enable more effective information sharing, coordination, and progress in the standards arena. Participants identified the following R&D investment areas to better meet this need: development and use of applications that address and enable communities of interest; approaches to reduce and equitably distribute costs of collaboration; inventory of current state and establishment of adequate controls (trust); filtering and monitoring mechanisms to increase collaboration flexibility; and use of increased trials and info sharing forums.

- **Focus on application of hybrid networks to achieve "seamless mobility."** Participants emphasized the significant potential for hybrid and ad hoc networking approaches to

fundamentally enable seamless mobility. Meeting this future goal would require considerable commitment, effort, and focused R&D investment on communications system operability and interoperability, assured communications in an all-hazards environment, and MANET-based approaches to address spectrum management/interoperability challenges. Participants urged leveraging existing military MANET R&D to support commercial applications, analysis of transition and migration strategies from the current system security implementations to the next generation ad hoc networking security environment, and support of NS/EP assured communications through next generation MANET implementations to include identity management and security/quality of service capabilities.

The following table (Figure 8) clarifies the agenda for action discussed during the Wireless and Mobile Ad Hoc Network Applications breakout session. The summary breakout session slides can be found in their entirety in Appendix D.

Figure 8. Wireless and Mobile Ad Hoc Network Applications Agenda for Action

Research Area	Recommended Focus
Identify and address human factor barriers to increased R&D to include cultural, governance, jurisdiction, and trust issues	• Identity management for "global, dynamic, technology-agnostic, hierarchical, meshed networks" • Use of technologies and capabilities that enable communities of interest • Full consideration of human factors in technology development, planning, and exercises
Open doors to foster collaboration, innovation, information sharing, R&D sharing and coordination, and standards and policy development	• Development and use of applications that address and enable communities of interest • Approaches to reduce and equitably distribute costs of collaboration; inventory of current state; and establishment of adequate controls (trust) • Filtering and monitoring mechanisms to increase collaboration flexibility • Use of increased trials and info sharing forums
Focus on application of hybrid networks to achieve "seamless mobility"	• Communications system operability and interoperability • Assured communications in an all-hazards environment • MANET-based approaches to address spectrum management/interoperability challenges

4.6 Breakout Session Summary

The following table (Figure 9) summarizes and clarifies several themes that spanned across the issues discussed in the individual breakout sessions.

Figure 9. Summary of Breakout Session Themes Matrix

	Global-Scale Identity Management	International Internet Governance	Collaborative Mechanisms	Cross-Border & Cross-Sector Challenges	Mobile and Ad Hoc Network Applications
Enabling Trust	Building circles of trust; increasing confidence across domains	Lack of international trust mechanisms for next generation technology	Trust between and among participants	Promote trust through improving information-sharing processes	Technologies and mechanisms to address and enable communities of interest
Information Sharing	Cross-recognition of practices; transferring credentials	Real-time sharing; data collection for incident response and cyber crime enforcement	Amending legislative and regulatory barriers	Balance between sharing and protecting proprietary considerations	Increase forums, trials, test cases involving international collaboration; foreign disclosure
Economic Justification	Exploration of cost models, business cases, and usability	Balance between public and private sector interests	Developing a value proposition; determining ratio between investment and profit	Need for incentives; determine expenditures based on risk and probability	Business case for non-military use; cost for collaboration
National Security	Defining national security requirements through scenario development	Implications of convergence on national security	Mechanisms to support national security	Interdependency studies to address national security concerns	Wireless and mobile applications to national security
Common Frame-works	Trust, risk and assurance agreements; common taxonomy; international standards	Common governance mechanisms to achieve multilateral cooperation	Facilitating cooperation through mutual agreements	Frameworks to establish effective cross-border collaboration	Multinational standards
Education, Awareness & Training	Identifying "Centers of Excellence"; improving awareness	Need to catalog existing international governance mechanisms	Creating awareness of related initiatives; leveraging best practices	Developing an inventory of existing initiatives; increasing qualified personnel	Increased training; leverage military applications

5.0 CLOSING PLENARY SESSION

The closing plenary session of the RDX Workshop began 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 six themes that spanned across all sessions:

- **Technologies and mechanisms to enable trust and build communities of interest are needed.** Enhanced security on the global communications network is dependent on an ability to interpret the trustworthiness of infrastructure, users, and devices. Several factors, such as human error, the need for commercial efficiencies, effective security policies and procedures, and personnel security and background checks, influence how trust is embedded in systems. The current network environment lacks universal applications and exercised processes and practices that allow parties to establish a high degree of confidence in the legitimacy and reliability of their counterparts, thereby stifling the development of functional communities of interest. Confidence and trust are jeopardized by a host of threats (such as exploitation by insiders, physical destruction). To enable inter-domain trust, users and devices must be able to develop, transfer, and accept identities and credentials through systems and solutions that provide for cross-recognition.

- **International collaboration is essential for successful cyber security R&D initiatives.** Current collaboration is limited and localized. R&D partnerships need to be created to promote cooperation and interoperation across borders, infrastructures, sectors, and domains. To effectively address the compelling network security risks that threaten economic sustainability, national security, and public safety, information sharing forums and mechanisms are essential for exchanging information and conducting collaborative R&D activities are imperative. Legislative and regulatory barriers need to be amended and incentives need to be created to facilitate appropriate levels of information sharing and international cooperation.

- **To advance cyber security research, leaders and practitioners must make investment decisions based on cost benefit analyses.** Recent innovations and advancements in networked information systems have brought about dynamic change, driven primarily by commercial forces. However, the security paradigm has not shifted to accommodate this evolving environment, thereby thwarting long-term progress. Future cyber security R&D proposals must address the cost of collaboration, articulate the value proposition, and include relevant business cases. To accomplish a posture of improved security and trustworthiness, strategies should be devised to leverage industry investments while accommodating market drivers; balance directives and incentives to stimulate progress; and blend influence and action to develop the next generation of security tools and products.

- **To maintain the current security posture and improve future preparedness and response, NS/EP requirements must be embedded in new technologies and methodologies.** The rapid pace of technological advancement demands increased focused on the importance of ensuring the resiliency, reliability and security of critical communications. Additional research on NS/EP scenarios and requirements is needed, as well as further development of existing systems and technologies that may have NS/EP applications. Future cyber security R&D must also consider how potential market decisions and economic impacts affect the security of free nations. New tools and services must incorporate NS/EP requirements during the pre-R&D stages and must continue to consider NS/EP implications through technology deployment and commercial adaptation.

- **Dynamic leadership and common frameworks are critical to achieve real progress in cyber security R&D.** General agreement on the set of "grand challenges" is needed to achieve larger goals and to encourage cross-border and cross-sector partnerships. Such vision serves to encourage collaboration, justify expenditures, and build global communities of interest around cyber security R&D. In addition, a common taxonomy enables different parties to clearly define priorities. While multinational standards efforts facilitate the development of common frameworks, cross-sector agreement on a roadmap for future R&D expenditures is also vital.

- **Strengthened education, awareness, and training programs increase the effectiveness of R&D partnerships and programs.** By improving knowledge sharing, members of the research community will be able to leverage best practices and related initiatives to enhance the effectiveness of current and future R&D investments. The critical challenge is to develop an R&D strategy that engages industry, Government, and academia, as well as end-users in exchanging information about existing initiatives and successes, thereby ensuring consideration of the full range of critical issues and facilitating the development of comprehensive, holistic solutions collectively. To inform the development of requirements and priorities, it is necessary to maintain an inventory of ongoing activities and to create linkages between centers of excellence across the world.

A question and answer period followed the breakout session presentations, with inquiries posed by the co-moderators and Workshop attendees. The question and answer period provided an opportunity for Ms. Sauvé-McCuan and Mr. Grimes to offer additional commentary on the issues raised during the breakout sessions.

In response to discussion on identity management, Ms. Sauvé-McCuan suggested the breakout session summary indicated a change in the identity management paradigm — one in which the focus had turned from trust to mistrust. Additionally, she suggested that Centers of Excellent be identified as a first step to achieving results and pinpointing solutions for identity management. Mr. Grimes concurred and reiterated the importance of identity management given its reach into all components of the network.

Following the discussion of cross border and cross sector challenges, Ms. Sauvé-McCuan raised the challenges associated with international partnering from a Governmental perspective but emphasized the value of sharing information and partnering given the global nature of the growing infrastructure. Mr. Grimes inquired as to the regulatory aspects of cross-border

partnering and the challenges of multi-national ownership of the telecommunications infrastructure. In response, the facilitators outlined the roles and responsibilities of the Committee on Foreign Investments in the United States (CFIUS) and agreed that the Committee provides sufficient protection of national security interests in multi-national ownership situations.

In response to discussion on the development of international collaborative mechanisms, Mr. Grimes suggested that the International Space Station represents an additional example that could be considered for influencing the style and design of a future R&D network security mechanism. In response to a question from a participant about the future management of global identities on the telecommunications network, the facilitator envisioned a parallel universe with two telecommunications networks — one free and open to all users like the current Internet and one that is highly managed with authenticated transactions and identity governance. He noted that the seeds of this are already in place via bank and Government transactions but doubted that the open Internet would be ever be removed due to the freedom and anonymity provided to users. In response to a question about the consideration of existing R&D Governmental agreements during breakout session discussion, the facilitator acknowledge that the group's participants were all aware of these agreements and did not ignore them during conversation, but they were intentionally not used as a starting point in order to stimulate free form discussion.

Following the breakout session presentations, Mr. Copeland invited Ms. Sauvé-McCuan and Mr. Grimes to offer closing remarks.

Ms. Sauvé-McCuan thanked Workshop participants for their diligent work and outlay of effort. She closed by highlighting the importance of communications networks that keep warfighters abroad safe. Ms. Sauvé-McCuan noted the need to ensure that information can be accessed and shared. Mr. Grimes also expressed his gratitude to participants for their focused work over the two-day event. He reiterated Ms. Sauvé-McCuan's comments, stating his priority is ensuring that warfighters can communicate and collaborate effectively. Mr. Grimes noted that he appreciated the opportunity to engage with participants on issues that are critical to the economy, the operation of the Nation, and emergency preparedness and restoration. In closing, he thanked Mr. Copeland for orchestrating the event.

Mr. Copeland concluded the 2006 RDX Workshop by thanking Mr. Grimes and Ms. Sauvé-McCuan for their personal engagement; the breakout session facilitators for guiding discussion and developing cogent, actionable recommendations; the invited speakers for offering valuable information and insights; colleagues from Industry Canada for taking equal ownership for the event and bringing an international audience together; the Crowne Plaza staff for exemplifying Canadian hospitality; participants for their dedication and hard work; and the Workshop planners for orchestrating another successful event.

Mr. Chaouki Dakdouki, Director, Regulatory Policy and Planning, Industry Canada, also offered his thanks to Mr. Copeland for bringing the RDX Workshop to Ottawa and sharing experiences and knowledge with Canadian colleagues. Before closing, Mr. Copeland emphasized the importance of staying engaged on these issues, taking actions to implement recommendations, and continuing to build and strengthen relationships and partnerships.

APPENDIX A

AGENDA

2006 RESEARCH AND DEVELOPMENT EXCHANGE WORKSHOP

International Collaboration on Cyber Security Research and Development:
Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response

Thursday, September 21, 2006

7:00 – 8:00	a.m.	Registration/Continental Breakfast at the Crowne Plaza Ottawa
8:00 – 12:00	***a.m.***	***Opening Plenary Session***
8:00 – 8:10	a.m.	Welcome/Introduction – Mr. Guy Copeland, Vice President of Information Infrastructure Advisory Programs, Computer Sciences Corporation, and Chair of the National Security Telecommunications Advisory Committee's (NSTAC) Research and Development Task Force
8: 10 – 8:15	a.m.	Introduction of Mr. John Roese, Chief Technology Officer, Nortel – Mr. Copeland
8: 15 – 8:25	a.m.	Welcome/Introduction – Mr. Roese
8:25 – 8:30	a.m.	Introduction of Ms. Patricia Sauvé-McCuan, Assistant Deputy Minister, Information Management, Department of National Defence – Mr. Roese
8:30 – 8:50	a.m.	Keynote Address from Ms. Sauvé-McCuan
8:50 – 8:55	a.m.	Introduction of Mr. John Grimes, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, Department of Defense – Mr. Copeland
8:55 – 9:15	a.m.	Keynote Address from Mr. Grimes
9:15 – 9:20	a.m.	Introduction of Dr. Anthony Ashley, Director General, Defense Research and Development Canada – Ottawa, Centre for Security Science – Mr. Roese
9:20 – 9:45	a.m.	Address on Key Canadian Research & Development (R&D) Initiatives Related to National Security and Emergency Preparedness Communications – Dr. Ashley
9:45 – 10:05	a.m.	Coffee Break
10:05 – 10:10	a.m.	Introduction of Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, Department of Homeland Security (DHS) – Mr. Copeland
10:10 – 10:35	a.m.	Address from Mr. Stephan
10:35 – 10:40	a.m.	Introduction of Dr. Douglas Maughan, Program Manager for Cyber Security R&D, Homeland Security Advanced Research Projects Agency, Science and Technology Directorate, DHS – Mr. Copeland
10:40 – 11:05	a.m.	Presentation on Current Cyber Security R&D Initiatives at DHS – Dr. Maughan

11:05 – 11:10 a.m. Introduction of Dr. Annabelle Lee, National Cyber Security Division, and Dr. Simon Szykman, Director, National Coordinating Office for Networking and Information Technology R&D – Mr. Copeland

11:10 – 11:35 a.m. Presentation on the U.S. Government R&D Planning Efforts for Communications and Cyber Security – Dr. Lee & Dr. Szykman

11:35 – 11:55 a.m. Introduction of Breakout Sessions & Concluding Remarks – Mr. Copeland

12:00 – 1:00 p.m. ***Lunch***

12:15 – 12:20 p.m. Introduction of Mr. Michael Zafirovski, President and Chief Executive Officer (CEO), Nortel – Dr. Peter Fonash, Deputy Manager, National Communications System, DHS

12:20 – 12:45 p.m. Address from Mr. Zafirovski

1:00 – 5:00 p.m. ***Breakout Sessions***

- Global-Scale Identity Management
- International Internet Governance
- Collaborative Mechanisms for Network Security Protocol R&D
- Wireless and Mobile Ad Hoc Network Applications
- Cross-Border and Cross-Sector Challenges

2:30 – 3:30 p.m. Refreshments

Friday, September 22, 2006

7:30 – 8:30 a.m. Registration/Continental Breakfast at the Crowne Plaza Ottawa

8:30 – 11:40 a.m. ***Breakout Sessions (Continued)***

- Global-Scale Identity Management
- International Internet Governance
- Collaborative Mechanisms for Network Security Protocol R&D
- Wireless and Mobile Ad Hoc Network Applications
- Cross-Border and Cross-Sector Challenges

10:00 – 10:30 a.m. Coffee Break

11:45 – 12:45 p.m. ***Lunch***

12:00 – 12:05 p.m. Introduction of Ms. Veena Rawat, President, Communications Research Centre Canada -- Mr. Fonash

12:05 – 12:30 p.m. Address from Ms. Rawat

1:00 – 3:30 p.m. ***Closing Plenary Session Moderated by Ms. Sauvé-McCuan & Mr. Grimes***

1:00 – 2:00 p.m. Facilitator Reports on Breakout Sessions

2:00 – 2:50 p.m. Question and Answer Period

2:50 – 3:05 p.m. Plenary Closing Remarks – Ms. Sauvé-McCuan

3:05 – 3:20 p.m. Plenary Closing Remarks – Mr. Grimes

3:20 – 3:30 p.m. Workshop Closing Remarks – Mr. Copeland

APPENDIX B

ATTENDEES

Attendees

Michael Aisenberg	VeriSign, Incorporated
Mike Alagna	Motorola, Incorporated
Shawn Anderson	Raytheon Company
Anthony Ashley	Defence Research and Development Canada
Bruce Averill	United States Department of State
Andy Bach	Securities Industry Automation Corporation
David Barron	BellSouth Corporation
James Bean	Verizon Communications, Incorporated
Gwen Beauchemin	Public Safety and Emergency Preparedness Canada
Cam Boulet	Defence Research and Development Canada
Stuart Brindley	Independent Electricity System Operator
Jim Brookes	Mathematics of Information Technology and Complex Systems, Incorporated
Ian Bryant	Central Sponsor for Information Assurance, United Kingdom Cabinet Office
Mitchel Butikofer	Office of the Assistant Secretary of Defense, Networks And Information Integration
Roger Callahan	Bank of America Corporation
Agnes Chan	Northeastern University
Paul Cheshire	AT&T, Incorporated
David Chinn	National Communications System/Department of Homeland Security
Stanley Chow	Alcatel Canada
Erin Comer	Booz Allen Hamilton
Kathryn Condello	George Mason University
Joseph Conti	Department of National Defence
Guy Copeland	Computer Sciences Corporation
Mike Corcoran	National Infrastructure Security Coordination Centre
Shawn Cormier	Communications Security Establishment
Pat Cottrell	Nortel Networks Corporation
Mario Couture	Defence Research and Development Canada
Robert Crawhall	Ontario Research Network for Electronic Commerce
Basil Crozier	Public Safety and Emergency Preparedness Canada
Chaouki Dakdouki	Industry Canada

David Darling	Natural Resources Canada
Shelly Davis	Booz Allen Hamilton
Michael De Jong	Public Safety and Emergency Preparedness Canada
Craig Delmage	Entrust Incorporated
Marc DesRosiers	Nortel Networks Corporation
David Dobbs	Northrop Grumman Corporation
Michael Doucet	Communications Security Establishment
Chris Dugal	Nortel Networks Corporation
John Edwards	Nortel Networks Corporation
Monte Egeland	Altobridge
Chris Ensor	National Infrastructure Security Coordinating Centre
Thomas Falvey	National Communications System/Department of Homeland Security
Melissa Fama	Industry Canada
Perry Fergus	Booz Allen Hamilton
William Ferguson	Carnegie Mellon University
José Fernandez	Ecole Polytechnique
Larry Finkelstein	Northeastern University
Mike Fitzgerald	Altobridge
Harry Fletcher	IHF Data Systems Incorporated
Peter Fonash	National Communications System/Department of Homeland Security
Nicholas Fong	National Research Council Canada
Reg Foulkes	Computer Sciences Corporation
Paul Frew	Motorola Canada Ltd.
William Fuller	National Communications System, Department of Homeland Security
Inette Furey	National Communications System, Department of Homeland Security
Robert Garigue	Bell Canada
Andrew Gebhardt	Department of National Defence
Kiesha Gebreyes	National Communications System/Department of Homeland Security
Seymour Goodman	Georgia Institute of Technology
Brenton Greene	Lucent Bell Labs
John Greenhill	Department of Energy, National Communications

	System/Departement of Homeland Security
John Grimes	Department of Defense, Networks and Information Integration
Allison Growney	Sprint Nextel Corporation
Elizabeth Hart	Booz Allen Hamilton
Gerald Harvey	Lockheed Martin Corporation
Brigitte Hébert	Communications Security Establishment
Ronda Henning	Harris Corporation
Marc Johansen	Boeing Company
Julie Kabous	Motorola, Incorporated
Henry Kluepfel	Science Applications International Corporation
John Kluver	Industry Canada
Ronald Knode	Computer Sciences Corporation
Ken Kuehni	Nortel Networks Corporation
Margaret Lackey	Industry Canada
Charles Lancaster	National Communications System/Department of Homeland Security
Bob Leafloor	Industry Canada
Andre Leduc	Industry Canada
Annabelle Lee	National Cyber Security Division, Department of Homeland Security
Julie Lefebvre	Defence Research and Development Canada
Steve Lloyd	Microsoft Canada Corporation
Stephan Maine	Third Brigade Inc.
Susan Maraghy	Lockheed Martin Corporation
Maneck Master	Telcordia
Douglas Maughan	Homeland Security Advanced Research Projects Agency/Department of Homeland Security
Andrew McAllister	Public Safety and Emergency Preparedness Canada
Michael McAllister	Dalhousie University
William McCrum	Industry Canada
Ernest McDuffie	National Coordination Office for Networking Information and Technology Research and Development
John Meincke	Unisys Corporation
Ali Miri	University of Ottawa
John Moore	Canadian Cyber Incident Response Centre

Marc Moreau	Royal Canadian Mounted Police
Tim Moses	Entrust Incorporated
Stephan Neville	University of Victoria
Thad Odderstol	National Communications System/Department of Homeland Security
Jack Oslund	George Washington University
Paul Pagetto	Public Safety and Emergency Preparedness Canada
Christine Pommerening	George Mason University
Gilles Racine	Nortel Networks Corporation
Veena Rawat	Communications Research Centre Canada
John Regnault	British Telecom
Lewis Robart	Industry Canada
John Robinson	Communications Research Centre Canada
John Roese	Nortel Networks Corporation
Alberta Ross	National Communications System/Department of Homeland Security
Marek Rusinkiewicz	Telcordia
Anthony Rutkowski	VeriSign, Incorporated
William Ryan	National Communications System/Department of Homeland Security
Marcus Sachs	SRI International
Mazda Salmanian	Defence Research and Development Canada
Patricia Sauvé-McCuan	Department of National Defence
Kay Scarborough	Eastern Kentucky University
Nabil Seddigh	Solana Networks
William Semancik	Department of Defense
Lee Shields	Royal Canadian Mounted Police
David Shinberg	Lucent Bell Labs
Jan Skora	Industry Canada
Jack Smith	Office of the National Science Advisor, Privy Council Office
Thomas Snee	Qwest Communications International, Incorporated
Julie Spallin	Canadian Cyber Incident Response Centre
Robert Stephan	Department of Homeland Security
John Stogoski	Sprint Nextel Corporation

Gretchen Sund	Booz Allen Hamilton
Tim Symchych	Communications Research Centre Canada
Simon Szykman	National Coordinating Office for Networking and Information Technology R&D
Helen Tang	Defence Research and Development Canada
Louise Tucker	Telcordia
Rod Wallace	Nortel Networks Corporation
Ian Walter	Altobridge
Dennis Weiss	Electronic Warfare Associates, Canada Ltd.
Mike Zafirovski	Nortel Networks Corporation
Steve Zeber	Defence Research and Development Canada
Marcus Sachs	SRI International
Mazda Salmanian	Defence Research and Development Canada
Patricia Sauvé-McCuan	Department of National Defence
Kay Scarborough	Eastern Kentucky University
Nabil Seddigh	Solana Networks
William Semancik	Department of Defense
Lee Shields	Royal Canadian Mounted Police
David Shinberg	Lucent Technologies, Bell Lab Innovations
Jan Skora	Industry Canada
Jack Smith	Office of the National Science Advisor, Privy
Thomas Snee	Qwest Communications
Julie Spallin	Canadian Cyber Incident Response Centre
Robert Stephan	Department of Homeland Security
John Stogoski	Sprint Nextel
Gretchen Sund	Booz Allen Hamilton
Tim Symchych	Communications Research Centre Canada
Simon Szykman	National Coordinating Office for Networking and Information Technology Research and Development
Helen Tang	Defence Research and Development Canada
Louise Tucker	Telcordia
Rod Wallace	Nortel Networks Corporation
Ian Walter	Altobridge
Dennis Weiss	Electronic Warfare Associates, Canada Ltd.
Mike Zafirovski	Nortel Networks Corporation

Steve Zeber	Defence Research and Development Canada

APPENDIX C:

SPEAKERS' REMARKS

Keynote Address
Mr. Mike Zafirovski

Remarks by Mike Zafirovski, President and Chief Executive Officer of Nortel
Research and Development Exchange (RDX) Workshop
Ottawa, Ontario, Canada, September 21, 2006

A "Boots on the Ground" Perspective:
What My Customers Are Doing That Makes Your Work So Crucial

Thank you for the gracious introduction, Dr. Fonash, and to all of you who put in the work to make this gathering happen.

And thank you to those of you who will be doing the important work over the next two days to firm up our industry's and our countries' approach to network security.

Looking through the audience, I see representatives of some of Nortel's best customers—many of the top carriers who are entrusted with the networks upon which the North American economy rides. But I also see some of our most worthy competitors and members of the academic community, the U.S. Department of Homeland Security, the Canadian Government, and of course other companies.

That's the power of this organization. NSTAC has a long and proud tradition of bringing together the best in breed to work on challenges we all face together. It's a model of how industry, Government, and academia should be cooperating. I thank you for your work.

Let me also welcome you to Canada and to Ottawa. This is a beautiful city, especially at this time of year, and it is home to Nortel's largest single concentration of R&D brainpower, which is why I am honored to speak to you for a few minutes before you get back down to the important business you have before you this afternoon and tomorrow.

Your choice of location is, in itself, symbolic. This is, as I understand it, the first meeting of this group outside of the United States. And that's the point of many of my remarks this afternoon. We all face a mutual challenge. We live in a global economy, and our communications systems are global.

Today's converging next generation networks make worldwide communications instantaneous. They put critical Government and business applications onto shared networks. They don't respect national borders very well. These are, of course, all clichés. I'm not telling you anything new here.

Yet everybody in this room can come up with their own communications horror story—relief groups arriving in New Orleans with incompatible telecom equipment or the suspicion that U.S. and Canadian border agents facing each other a couple of hundred yards apart might have trouble communicating in a crisis.

In spite of all the media attention to cyber security, one recent study of Wi-Fi networks in London, Frankfurt, New York, and San Francisco showed that more than 33 percent of the companies using them had turned their security features off.

The health of Nortel's business, our customers' businesses, the businesses and agencies you work for—and our respective nations—depends on the work you do as you dig deeply over the next two days into how we deal with security threats to the global, increasingly "cyberized" networks we all depend on.

Nortel Perspective:

Nortel has been an NSTAC member since 1983, almost since the beginning.

We build robustness into the DNA of our equipment—it's an absolute tablestakes' customer requirement. We're known for bringing 5 9's reliability to our carrier customers. And over the last year we've made Lean Six Sigma a key part of our business plans to ensure we keep improving that robustness and quality.

What we like to refer to as Roese's Law (somewhat jokingly named for our new CTO) guides every product decision at Nortel—"There are no security-agnostic entities—every technology, every piece of hardware or software, either augments or weakens security of the overall network".

Being a global company, we also very much feel the increasing demands for global security and have been very active in multiple efforts to bring about alignment and interoperability in the emerging telecommunication technology areas.

An example of this is the T1.276 standard that we edited within the Network Security Information Exchange in the U.S. and subsequently published through ATIS. It has now been adopted by ITU and ETSI in the European Union.

We are an active member in the international security standards arena, where work is in progress to extend security recommendations to the Signaling and Media planes of the network.

We have recently extended the inherent capabilities of WiMAX with a holistic Layered Defense model that further secures applications sent across the network

We understand the need for Global-Scale Identity Management as credentials for First Responders and other users increase into unmanageable numbers

We understand the role that Governments can play in stimulating the right R&D in cyber security research.

Everyday, we live the cross-border and cross-sector challenges one of your groups will be taking on in this afternoon's R&D Exchange.

We are deeply interested, in fact, in all five areas you will be working on for the next two days

How can I be of most value to you in the few minutes before dessert arrives and then you go back to your work?

I think I can probably spend that time best by telling you what our customers are saying to me everyday. Where they see their next generation networks going. Where they tell me they will be spending their money in the next few years. This is where Nortel as a company is placing its R&D bets. So, here's my "boots-on-the ground" perspective.

I've talked to hundreds of customers over the last nine months. Here are my key findings:

Each should drive how we as a security community need to be thinking about the future.

First, Mobility and Convergence are driving next generation networks.

We know, for instance, that video–especially mobile video–is going to dramatically change today's networks.

A quick study at Nortel makes us think that if less than 10 percent of most of mobile users begin to demand true broadband wireless—the kind required for mobile video, for example—even the best 3G networks would quickly be in trouble. A couple of weeks ago, Apple announced its new iTunes video initiative, which they promise will also soon be delivered on wireless networks. 4G networks are going to take off--and much more critical data than music videos will soon be running on them.

When emergency response teams, for instance, can count on WiMAX connections at five times the rate of today's WiFi, the whole dynamic of what can be done on the ground with ad hoc emergency networks is going to change during a crisis like the one we saw with Katrina. 4G will be at the core of our security responses and our defense communications going forward.

Chuck Saffell, the head of our Government Solutions group, is in fact this morning addressing TechNet North in Ottawa. He is talking about what 4G technologies could do for the commander in the field if he or she had the bandwidth to set up secure video calls, send real-time video reconnaissance, transmit maps or visual directions via a hand-held device, and see real time visuals of their area of operations.

Second, IP has changed everything.

Networks are converging around it at unbelievable rates, and they are moving to data centers. This brings cost-effective standards, this allows many, many applications to run on flat networks, and this allows dramatic increases in business productivity.

But it also means that increasingly our traditional communications networks are exactly the "cyber" that is the topic of your discussions this afternoon. You can count on continuing to see telecommunications moving towards IP in exponential ways—and carrying with it a host of business-critical applications that once would have been totally segregated from traditional telecommunications networks.

We'll see not only huge movement in people-to-people traffic, but an increased emphasis on people-to-device, and device-to-device communications—much of which will be critical to the daily operations of businesses around the globe and to Government continuity in times of crisis.

Huge amounts of traffic will be centralized and flowing over the backhaul networks that connect wireless access points.

Third, 21st Century Governments and enterprises will be multimedia enabled and virtualized.

Our customers are moving forward very quickly to integrate their business applications with their telephony networks

And their businesses are becoming virtual, they expect their employees to have, for instance:

- Anytime, anywhere user connectivity;
- Ubiquitous broadband wireless;
- Wireless-wired equivalence;
- Data center consolidation; and
- Secure communications across trust domains.

They want to federate their networks out to their supply chain and expect airtight identity management and security.

Entire industries are going to spring up, for instance, around new network-connected appliances. Today's refrigerators, washers, dryers, surveillance cameras, and even pool pumps are coming equipped with network connections. We will more and more see the emergence of such devices, which will connect to any number of wired and wireless networks.

It's an inconvenience if your home appliance network fails. But if the system of chemical, biological, radiological, and nuclear sensors that will soon be efficiently and effectively monitoring shipyards, nuclear facilities, and key transportation routes goes, then we're facing an altogether more serious problem.

Bottom line: A threat to a virtualized business and Government is a threat to the very heart of our economies and our safety. It's not just the phones going out—it's the entire enterprise with all its call centers, its billing software, with its supply chain, all tied together and interdependent.

Fourth, let me address the Services and Solutions business.

A key indication of this rush to a converged, mobile, virtual world is the interest our customers are showing in asking service providers to plan, manage, and run their networks. A key part of our current business transformation is to provide the expertise that holds networks together. It's at the core of our new business model. It's that important.

Simply said, the global business and Government community will continue to capitalize on next generation networks. They are way too powerful to ignore. But the customers will want to concentrate on their core businesses, not their networks.

And their key concern is that the networks remain up and running under any scenario. There's an unease out there that they are willing to pay well to address. And teams like yours are key to driving and sharing the standards, certifications, best practices, and learnings that will allow us all to capitalize on these technologies.

Conclusion/Call to action

You each come here as experts in securing our networks. I expect that you are all quite familiar with the trends I've just gone through. I hope, though, that I've been able to underline for you just how quickly they are happening in the marketplace

How rapidly converging, mobile, and increasingly interconnected networks are changing how our societies work.

And how important it is that the security and robustness underlying them keeps up with the change. And how important it is that Government policy supports these efforts.

The work you have to do is real, and it is urgent.

You can, of course, continue to count on Nortel's continued subject matter expertise to NSTAC as it moves forward.

And I plan, in fact, to spend a good amount of time next week meeting with Canadian officials to discuss how to help firm up Canada's telecoms policy.

So I'm particularly happy to see NSTAC in Ottawa to emphasize the global nature of the challenges we all face together.

The industries and nations you serve need the work you are doing.

I am looking forward to fruitful collaboration and exchange over the next two days.

I can assure you that your final report will be key to NSTAC as it prepares advice to President Bush in the fall and trust that the Government of Canada and the global community will find the report useful as well.

Thank you for your good work and your time.

Keynote Address:
Ms. Patricia Sauvé-McCuan

Remarks by Ms. Sauvé-McCuan, Assistant Deputy Minister, Information Management, Department of National Defence
Research and Development Exchange (RDX) Workshop
Ottawa, Ontario, Canada, September 21,2006

I would like to start my remarks by thanking the National Security Telecommunications Advisory Committee for the invitation to participate with you in this Exchange. It is both a pleasure and a privilege to address this international forum devoted to collaboration on cyber security. I note that this is the first such RDX taking place outside the continental U.S. and I believe that this is a clear demonstration of the connectivity required between allies in furthering the exploration of common issues. Canada and the USA have a special relationship, one that has been forged in peace and reaffirmed with recent events. In fact, only ten days ago, we commemorated the fifth anniversary of the September 11th terrorist attacks, and I think that it is important to look to those events as the backdrop for this workshop, especially as it relates to securing our information assets. Without a robust, and more relevant to today and tomorrow's workshop, secure technological platform from which we can support operations, we are not providing our citizens, our Government, or our allies with the information support that is necessary to ensure operational supremacy.

As I reviewed the objectives of the conference, I was reminded of a TV channel's pitch—Television without Borders—and this brought to mind the issues relating to cyber security—the fact that there are no borders with respect to information flow. There are certainly no borders to cyber terrorists and we have to ensure through deliberations such as these that the appropriate tools are developed to deny and thwart any malicious intent.

As the Assistant Deputy Minister for Information Management in the Department of National Defence, my job is to ensure that information is accessible, transferable, and reliable and that it gets to the right person at the right time in the right form to enable them to make strategic, operational, and more and more so tactical decisions. Thus, my information role pervades the organization. Simply stated—information is the crux of what I do. Cyber threats are a risk to what I do—effective cyber security will mitigate that risk.

Imagine the following scenario, and I am certain all of you already have—power distribution in Toronto starts to fail sporadically and intermittently during the business day disrupting business but not causing a complete blackout of the sort that we experienced several years ago. Traffic begins to snarl as lights at intersections fail to the "four way flashing red" mode; the subway system becomes erratic because of power interruptions. The brief disruptions go on for hours and then days. A similar scenario repeats in major cities across North America. Disruptions are short and appear to be isolated but they start to affect business at the local level, spreading to the continental and then international level. There is no common set of symptoms and it takes days or weeks before national authorities identify the similarities of the disruptions. Is this a repeat of the failure of the power grid or is it the systematic disruption of the grid through the introduction of malicious codes into the controlling software? Regardless, the effect is the same—inconvenience initially, building to the disruption of business, and eventually significant

economic impact and potentially threatens public and personal safety, all the while with authorities devoting resources to finding the cause and in some cases, laying blame. This scenario speaks volumes to the need to detect and render useless all risk resulting in technological disruptions, whether self inflicted or unintentional, or terrorist attacks. Cyber threats take many forms but the commonality amongst them all is the risk of reduction in functionality or the outright denial of service. The electricity blackout on the eastern seaboard of a few years ago demonstrated the fragility of the very networked infrastructure that we must protect.

The 25th anniversary of the personal computer was only recently celebrated around the world. Many of us will remember the introduction of the IBM PC but it was really some 15 years earlier that the notion of a "wired world" was born. The Internet is less than 40 years old if you concede that it owes its origins to the DARPANET/ARPANET of the late 60's. While the visionaries who dreamed of a network that would connect businesses and individuals have seen their dream realized, in part by the introduction of the PC, who would have thought 40, 20, or even 10 years ago that we would be at risk for having our individual identities stolen by the same technologies that have enhanced our ability to research, communicate, and collaborate? This is the fastest growing crime sector in the western world today. I raise this point because it is this basic technology that is now in regular use by 70 percent of North Americans. While other areas do not enjoy quite the same penetration, it is clear that the developed nations are achieving in the neighborhood of 50 percent Internet penetration; and, industry has set a goal of global Internet penetration of fifty percent by 2015. This is an impressive goal given that current global penetration is less than 20 percent. But even at today's level of Internet exposure, we can see the challenges today in ensuring that our cyber world is safe, secure, and assured.

With this backdrop, I would like to provide a high-level assessment of the challenges that face the public and private sectors here in Canada, in North America, and certainly around the world. And that is probably the first point that I should make. Cyber security is a global issue. The threats to cyber capabilities are global in nature simply because of the pervasiveness of our networks and the interconnected nature of the Internet, private networks, shared, and connected networks as we see in the financial and utilities domains, and of course closed Government networks. I would offer that our closed, secure Government and military networks are not only the most secure because we have cryptography, procedures and practices, operated by highly trained, trusted users, but probably more importantly, because they aren't connected to the outside world without significant engineering solutions. What I am saying here is that our closed Government and defence networks are the most secure when they remain disconnected from other systems and networks. But we all know that the power of information is based on our ability to share it. So this is our dilemma—how do we assure the availability and security of our networks, while ensuring that we can connect, communicate, and collaborate? And when I talk about our networks, I am talking about the high-end C4ISR systems that are used by commanders in coalition warfare. I am talking about the systems that control the power grid to which the hundreds of hydro producers connect. I am talking about the systems that share information in support of cross-border travel and trade, the banking systems, the systems that deliver services to citizens, and of course, I am talking about the Internet. Our duty to share information must be balanced with our responsibility to protect information.

The Government of Canada and all of the Provinces and Municipalities use computer systems and networks extensively to manage information and offer services to Canadians. Many federal Government operations are now dependent on these technologies and on supporting critical infrastructures such as the Internet, the electrical power grid, and transportation and traffic management just to mention a few. However, this unprecedented level of automation and connectivity is challenging the development of security measures needed to protect these systems from cyber-attacks.

Canada's National Security Policy states that "the threat of cyber-attacks is real and the consequences of such attacks can be severe." The Communications Security Establishment is currently working to strengthen Government of Canada capabilities in order to defend against cyber threats.

The Federal Government is under nearly continuous attack by sophisticated intrusions into its computer systems. These intrusions resulted in minimal damage and, touchwood, have been always detected and defeated, but they could have been designed to be much more harmful than they were. If trends continue, more devastating attacks are likely to occur. The open and public nature of the Internet makes it vulnerable to an ever-increasing range of attacks that are relatively easy and inexpensive to execute. Hackers, malcontents, organized criminal elements, and foreign intelligence organizations are among a diverse array of cyber threat adversaries targeting electronically accessible information from Governments, businesses and households.

We need to understand that these individuals, agencies, and in some cases hostile Governments are benefiting from the relative low level of effort required to attack computer networks and compromise information and data. This relative simplicity in attacking networks is complemented by the quality and availability of attack tools and malicious codes. You are aware of the publicly accessible websites at which these tools can be found at little or no cost. Consequently, the frequency, speed, and complexity of attacks are rising exponentially. Because many incidents go either undetected or unreported and victims are often unable to determine the full extent of personal losses, it is difficult to estimate the total impact that cyber incidents are having in Canada or around the world.

While events like this bring interested and informed members of the public, Government, industry, and academia together to address this subject, awareness about cyber threats needs to be improved at the laypersons' level. The public needs to benefit from access to more information, in simple terms, complemented with better and more aggressive implementation of security measures both in public and private networks. There is no single solution for protecting all computer systems and networks. Multilayered security strategies will be needed to protect critical infrastructures from cyber-attacks. While Government bodies, agencies and Departments will identify and assist in securing the Government of Canada's computer systems, the responsibility to assure cyber security and ensure information access in Provincial, Municipal, industry, and private networks clearly lies with the system owners and operators. They must share their knowledge and approaches.

Notwithstanding that the organizations responsible for systems are also responsible to secure the systems, the real challenge is clearly to ensure that security is assured across the boundaries of interconnected systems or else, the resulting "system-of-systems" will only be as secure as the

weakest link. This development of standards is a key area for Government and industry cooperation and consultation. While Government bodies such as the Communications Security Establishment and the Royal Canadian Mounted Police have the skilled workforce and experience in information security to take a lead role in cyber protection, their responsibilities would typically be limited to cyber security within the Government of Canada but should also be used to advise the other sectors on both the IT provider and consumer sides to ensure that standards and products are developed to support national objectives for information protection.
In the aftermath of 9/11, Governments around the world dedicated more resources to counter foreign intelligence threats, to provide advice and guidance for the protection of Government information networks, and provide assistance to Federal law enforcement and security agencies. As much as being a reaction to the "new reality," this reassignment of resources has been an acknowledgement of the complex and complicated, multifaceted nature of cyber security and the need to collaborate with international allies and domestic partners to share information and develop solutions. It is especially important for Canada to work closely with the United States to protect shared North American infrastructures and services. Government departments and agencies and industry sectors, must work together nationally and internationally to improve threat and vulnerability analysis and expand Government capabilities to predict and prevent cyber attacks, including stronger defensive mechanisms on Government networks of most importance to minimize impact. Additionally, we must also find better means within which we can leverage each others solutions.

Our programs must be more than unilateral reactions to an attack. The cyber security strategy needs to improve capabilities for predicting, preventing, and minimizing damage from cyber attacks. To help predict future cyber attacks, research efforts must examine new tools and techniques in cyber security and forecasting and focus on predictive capabilities for cyber security that will help focus resources on the most significant threats. In addition to protecting its own systems, the Government's role should be to establish standards and promote the development of solutions to aid other public and private organizations in assessing the security of their computer networks and to offer advice and guidance on how to address vulnerabilities detected in their systems.

To minimize recovery times from cyber attacks that do occur, the Government should provide an IT "triage" function. In the wake of an attack, a technical assistance team could quickly determine how the attack took place and its potential origin. It could also prevent the spreading of the attack, and take mitigation measures to prevent the failure of critical infrastructure and services. With this knowledge, new protection solutions could be developed to improve the security of other vulnerable networks. Joint emergency planning and participation in exercises further help organizations prepare for a potentially severe cyber attack against Canada.

Several Federal Government departments have already established information protection operations centres to help defend their networks. These centres detect intrusions into systems and respond to cyber incidents when they occur. Industry should do likewise and potentially, user industries such as utilities and the IT industry could establish reactive protection centres to ensure the availability of critical services during a cyber attack. All organizations can reduce their exposure to cyber threats by considering IT security measures at the beginning of IT initiatives and projects. Federal departments should review their compliance with Federal

Government policies for security and further ensure that IT support centres adequately maintain system security and software patches.

Protecting the Government of Canada's most important information and critical cyber infrastructure is a huge challenge. As the number of threats, targets, and vulnerabilities grow, so must the ability to predict, prevent, and minimize damage from cyber attacks. However, there is a role for everyone in improving cyber security.

Some of you will be aware that the Government of Canada has established a Cyber Security Task Force within the department of Public Safety and Emergency Preparedness Canada. This move will go a long way to addressing implied shortcomings in Canada's cyber security framework. Indeed, its role is to develop the cyber security framework and to serve as Canada's focal point for dealing with cyber threats to Canada's critical infrastructure.

As the former Minister of Public Safety and Emergency Preparedness stated last year:
"In a global environment where we are increasingly reliant on information technology, we have a responsibility to do everything we can to reduce the risk of cyber threats that could have an impact on our shared critical infrastructure."

This new role for Public Safety and Emergency Preparedness Canada will not be without challenges. The first challenge will be to determine who will be consulted: the public, the IT industry, user industries, privacy and civil liberties groups? The office will also have to determine what legislative framework is necessary and possible to ensure that rules, policies and laws are enforceable; and finally, Canadians will want to know how the Task Force will protect them from fraud, spam, phishing, and spyware to prevent the massive consumer losses, and restore confidence in e-commerce and the Internet.

Alright, I would like to try to wrap this up now that I have given you a brief apercu of what I see as the issues and challenges and how the Government is preparing to address them. Cyber security used to be the business and the challenge of defence departments, intelligence agencies, and police forces. This is no longer the case. The Internet has put the challenge of cyber security squarely in the laps of everyone: Governments at all levels, the IT industry, the consumer industry (including service providers), and the end user—Jane Q Public. In brief, cyber security is everyone's problem and unless we take it seriously, we will leave ourselves open to attack and system failures that reach far beyond the information systems themselves.

There is a triad of tensions at work when we talk about common cyber security. The first element is the need to share. We need to share information and we need to share access. Whether we are talking about sharing secure information among various Federal agencies, or talking about Canada and the U.S. sharing information and access to databases to facilitate cross-border trade and traffic, or whether we are talking about connecting the myriad of utility control systems, we need to share information in a secure environment. Secondly, we need to protect our information and our systems. This can be in opposition to our need to share. We need to defend our systems in depth with hardware, software, practices, and procedures that assure both us and the organizations to which we connect. Our defence not only has to protect the defender but also those connected to the defender. Finally in this triad, when we address the need to share and the need to protect and assure the integrity of our systems, we need to consider the need and the

legislated right for privacy. There will be people and organizations that insist that the right to privacy is more important than the right to defend against a cyber attack. We may come close to compromising the rights of individuals when we attempt to achieve the desired level of cyber security. This balance needs to be understood, articulated, and validated by appropriate legal bodies.

Governments have a role to play in the cyber security of the Nation. First they need to defend and protect their own networks. Secondly, working with the IT industry, users, and service and utility providers they need to develop standards and solutions for others to follow. Cyber security will only be achieved through collaboration and cooperation at all levels.

The user industries, such as the utilities, need to work together to identify vulnerabilities and to share solutions. Similarly, they need to put aside competition in the business to collaborate for the good of the enterprise.

And finally, the user has a role to play in preventing, identifying, and mitigating vulnerabilities and attacks. The users are in the best position to understand the impact of the failure of their systems.

In closing, and I'm really wrapping up this time, the Government has achieved major strides in protecting its own systems and defending its own networks. The ongoing work to develop the cyber security framework will pay important dividends, not only in preventing system failures but also in preventing the loss of critical infrastructure. Cyber security starts with all of us—awareness, identification of the threat, prevention, and mitigation are our goals.

Information sharing exchanges such as this will focus our combined efforts to improving the cyber world. The world has changed dramatically since the cold war, when even school children could identify the threat back then. Today we are living in a world of constant change, asymmetric threats and one in which our enemy's whereabouts, identities, and tactics are undefined.

Information assets are essential in dealing with today's threats as well as emerging threats. Enhancement of cyber security capabilities is critical to our ability to detect and defeat these threats. All of us in this room have a large part to play in building our defence capability.

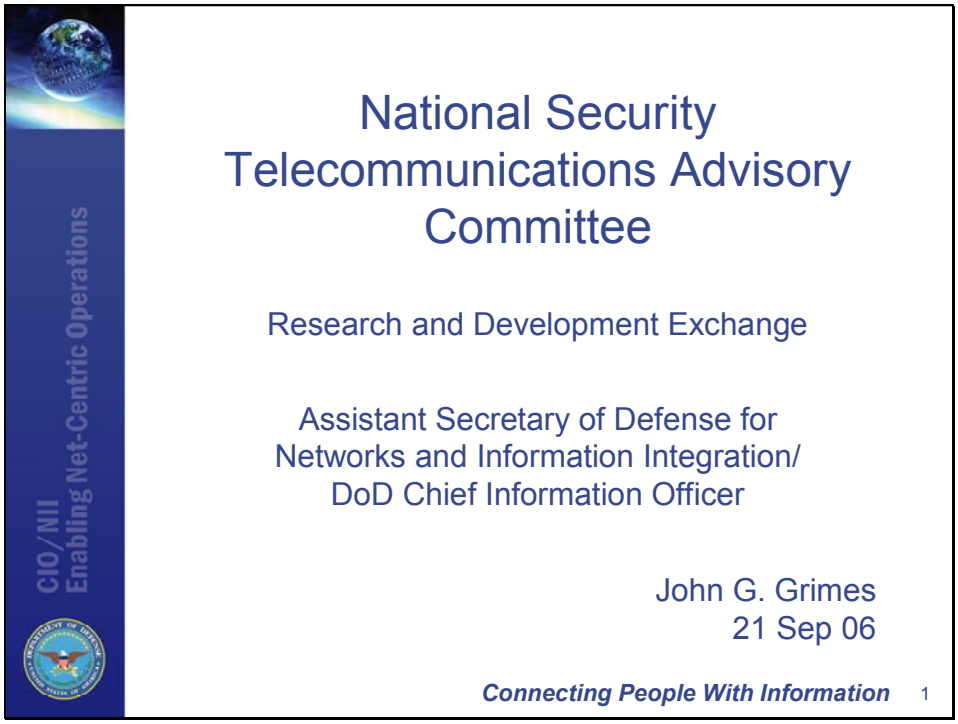
Over the next two days you will share key information and dialogue allowing all of us to move towards a more secure cyber environment.

Unfortunately, the exigencies of daily evolving priorities are calling me back to my headquarters and I am not able to hear much of this morning's dialogue with you. I will have to depart following John Grimes' remarks. I do look forward to hearing the fruits of your deliberations tomorrow afternoon and discussing the way ahead.

I wish you all a productive and rewarding two days. Thank you.

Keynote Address:
Mr. John Grimes

Remarks by Mr. Grimes, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, Department of Defense
Research and Development Exchange (RDX) Workshop
Ottawa, Ontario, Canada, September 21,2006



CIO/NII Enabling Net-Centric Operations

Transforming National Defense – Net-Centric Operations

National Security Strategy

Transform America's national security institutions to meet the challenges and opportunities of the twenty-first century.

National Defense Strategy

We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.

Beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes...

Transforming to a network-centric force requires fundamental changes in process, policy, and culture.

National Military Strategy

...creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations... on demand to defense policymakers, warfighters and support personnel.

Connecting People With Information 2

CIO/NII Enabling Net-Centric Operations

CIO Vision and Mission

Vision

Deliver the Power of Information

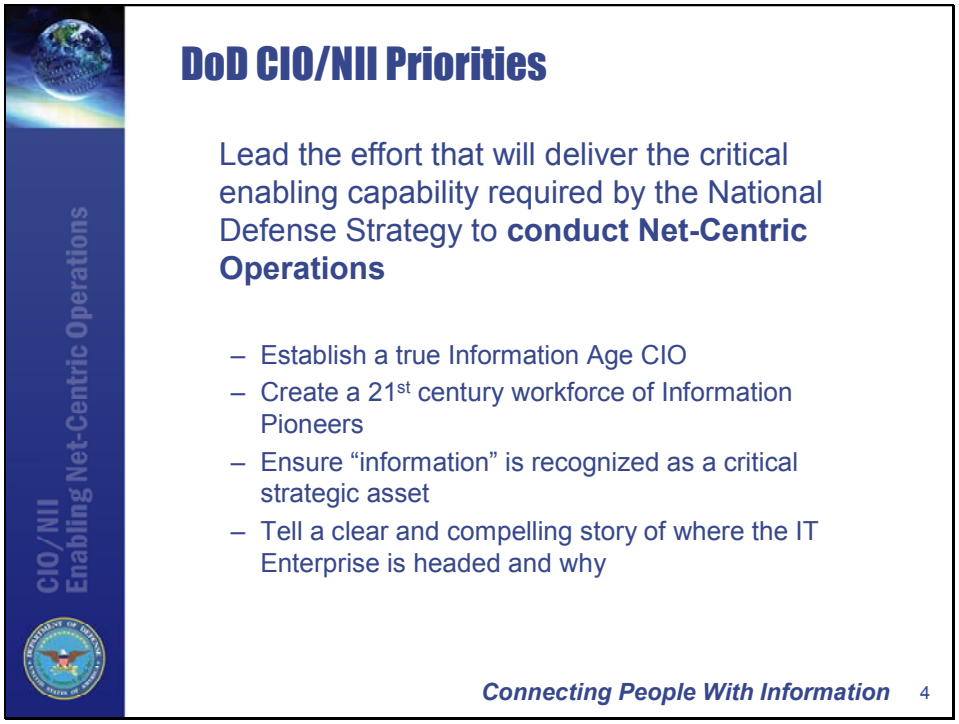
An agile defense enterprise empowered by access to and sharing of timely and trusted information

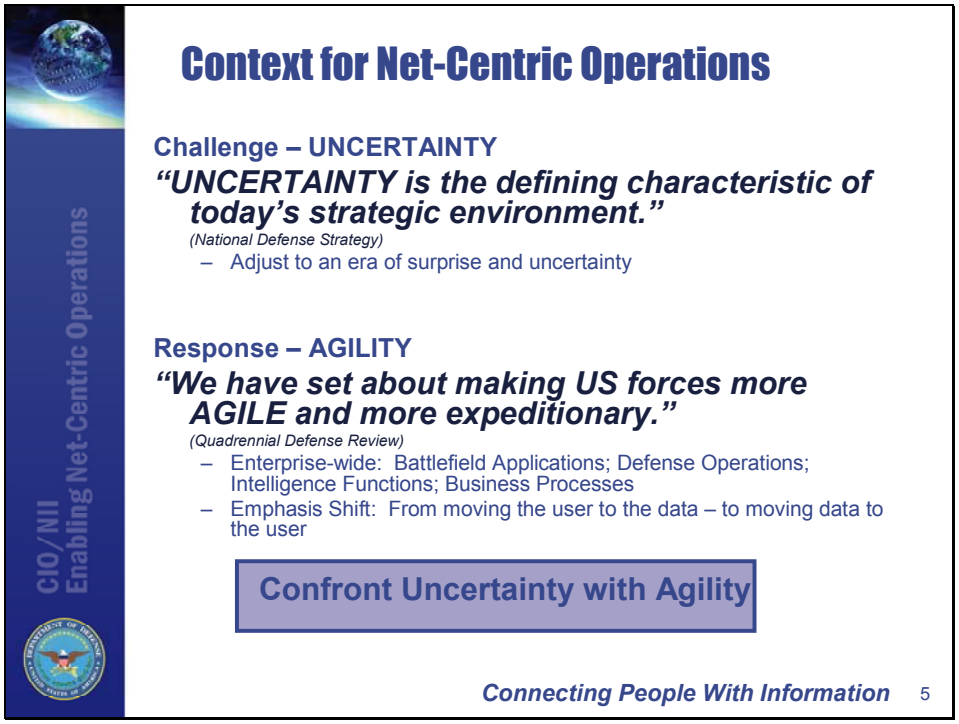
Mission

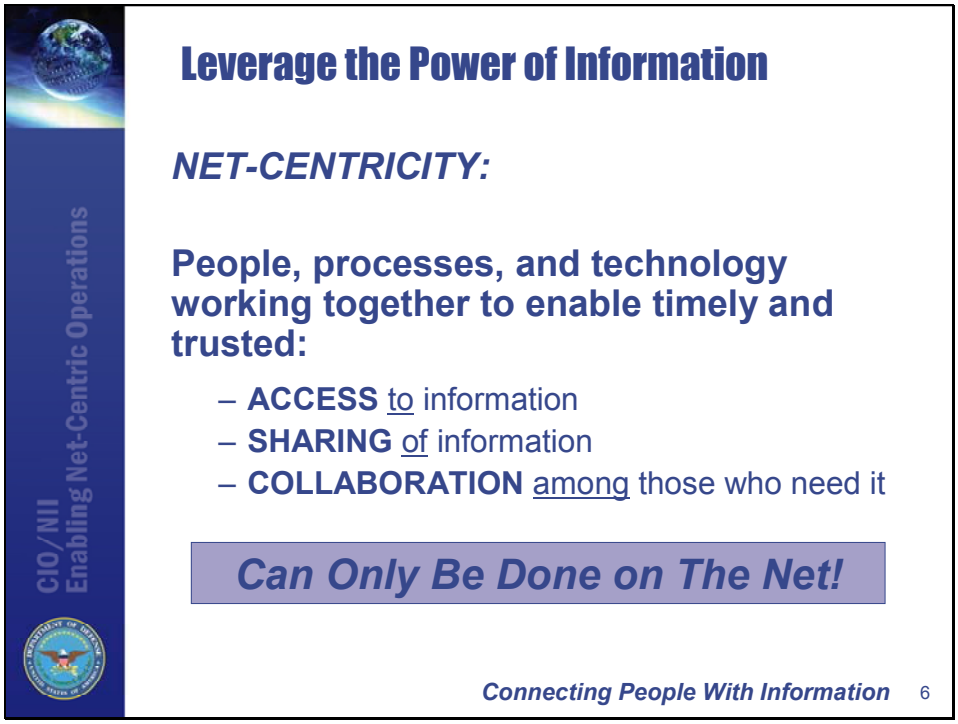
Enable Net-Centric Operations

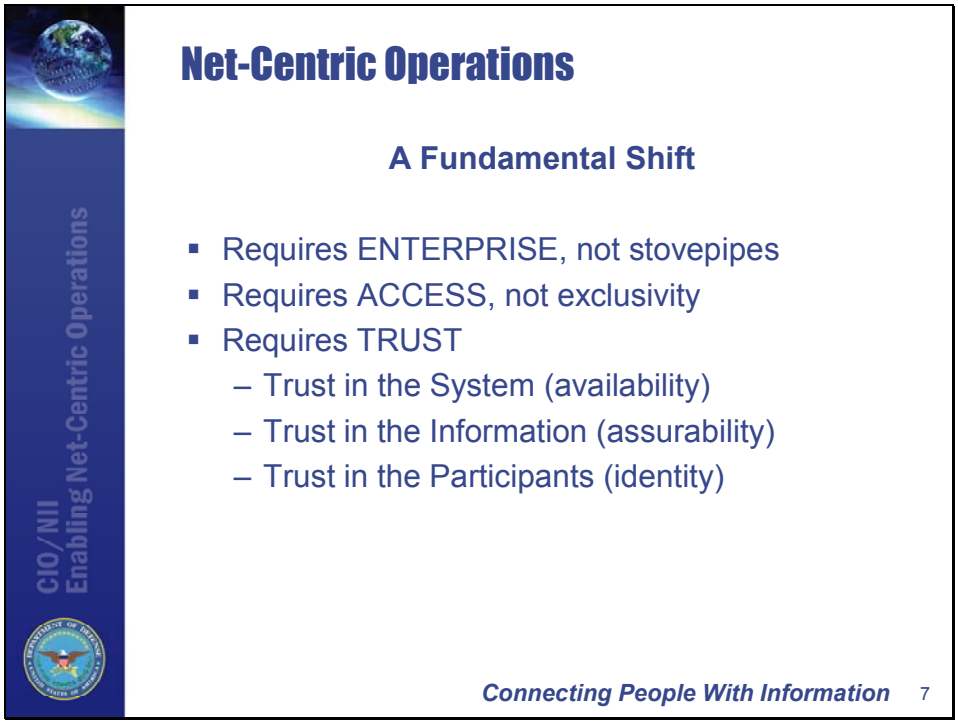
Lead the Information Age transformation that enhances the Department of Defense's efficiency and effectiveness

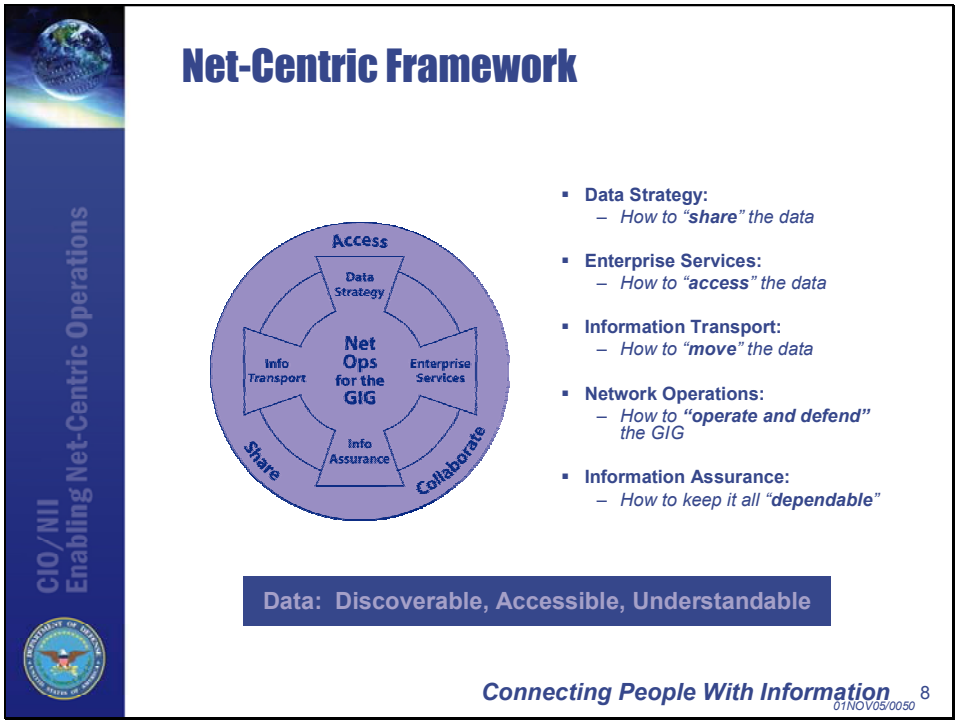
Connecting People With Information 3

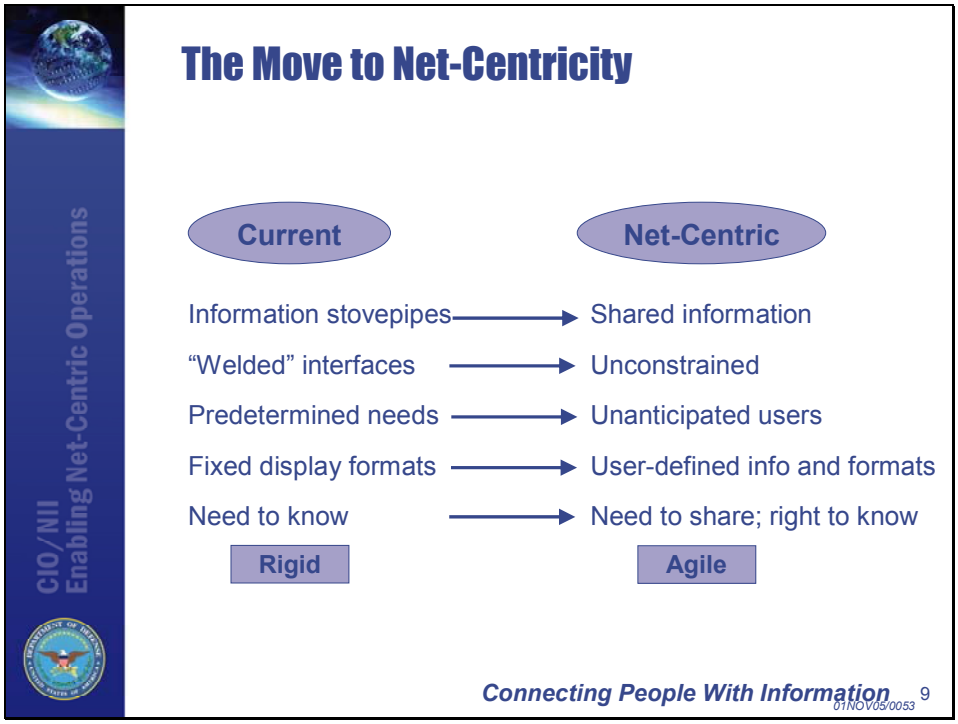

CIO/NII
Enabling Net-Centric Operations
DoD CIO/NII Priorities
Lead the effort that will deliver the critical enabling capability required by the National Defense Strategy to conduct Net-Centric Operations
– Establish a true Information Age CIO
– Create a 21st century workforce of Information Pioneers
– Ensure "information" is recognized as a critical strategic asset
– Tell a clear and compelling story of where the IT Enterprise is headed and why
Connecting People With Information 4


CIO/NII
Enabling Net-Centric Operations
Context for Net-Centric Operations
Challenge – UNCERTAINTY
"UNCERTAINTY is the defining characteristic of today's strategic environment."
(National Defense Strategy)
– Adjust to an era of surprise and uncertainty
Response – AGILITY
"We have set about making US forces more AGILE and more expeditionary."
(Quadrennial Defense Review)
– Enterprise-wide: Battlefield Applications; Defense Operations; Intelligence Functions; Business Processes
– Emphasis Shift: From moving the user to the data – to moving data to the user
Confront Uncertainty with Agility
Connecting People With Information 5


CIO/NII
Enabling Net-Centric Operations
Leverage the Power of Information
NET-CENTRICITY:
People, processes, and technology working together to enable timely and trusted:
– ACCESS to information
– SHARING of information
– COLLABORATION among those who need it
Can Only Be Done on The Net!
Connecting People With Information 6


CIO/NII
Enabling Net-Centric Operations
Net-Centric Operations
A Fundamental Shift
▪ Requires ENTERPRISE, not stovepipes
▪ Requires ACCESS, not exclusivity
▪ Requires TRUST
– Trust in the System (availability)
– Trust in the Information (assurability)
– Trust in the Participants (identity)
Connecting People With Information 7


Net-Centric Framework
CIO/NII Enabling Net-Centric Operations
Access
Data Strategy
Info Transport
Net Ops for the GIG
Enterprise Services
Info Assurance
Share
Collaborate
Data Strategy:
– How to "share" the data
Enterprise Services:
– How to "access" the data
Information Transport:
– How to "move" the data
Network Operations:
– How to "operate and defend" the GIG
Information Assurance:
– How to keep it all "dependable"
Data: Discoverable, Accessible, Understandable
Connecting People With Information
01NOV05/0050
8


The Move to Net-Centricity
CIO/NII Enabling Net-Centric Operations
Current
Net-Centric
Information stovepipes → Shared information
"Welded" interfaces → Unconstrained
Predetermined needs → Unanticipated users
Fixed display formats → User-defined info and formats
Need to know → Need to share; right to know
Rigid
Agile
Connecting People With Information
01NOV05/0053
9

CIO/NII Enabling Net-Centric Operations

Critical Technology Enablers

IPv6
- Supports proliferation of IP-addressed applications/devices, and "comm on the move"
- DoD Transition Strategy:
  - Tech Refresh

VOIP
- Increases flexibility/capacity through broadband Internet connection; allows for converged voice and data on the same network
- DoD Initiatives:
  - Developing standards to end-to-end VOIP capability

Satellite Communications
- Enables real time connectivity, high data rate, ISR exfiltration, and comm on the move
- DoD TSAT Program Restructure:
  - IOC 2013; 4 on orbit 2017

Mobile Communications
- Provides network entry device for individual users at the tactical edge
- DoD JTRS Program:
  - Joint Program Office established
  - Form-factors being developed

Service-Oriented Architecture
- Establishes easy-to-use services to access, share and collaborate
- DoD Strategy:
  - Acquire commercially managed service (NCES goal)

Information Assurance
- Assures DoD's information, information systems, and information infrastructure
- DoD Strategy:
  - Fundamental shift from "walls and patches" to "secure from the start"
- DoD Initiatives:
  - Build IA architecture
  - Expand partnership with industry for IA R&D

Connecting People With Information 10

CIO/NII Enabling Net-Centric Operations

"I can get the information I need"

When I need it

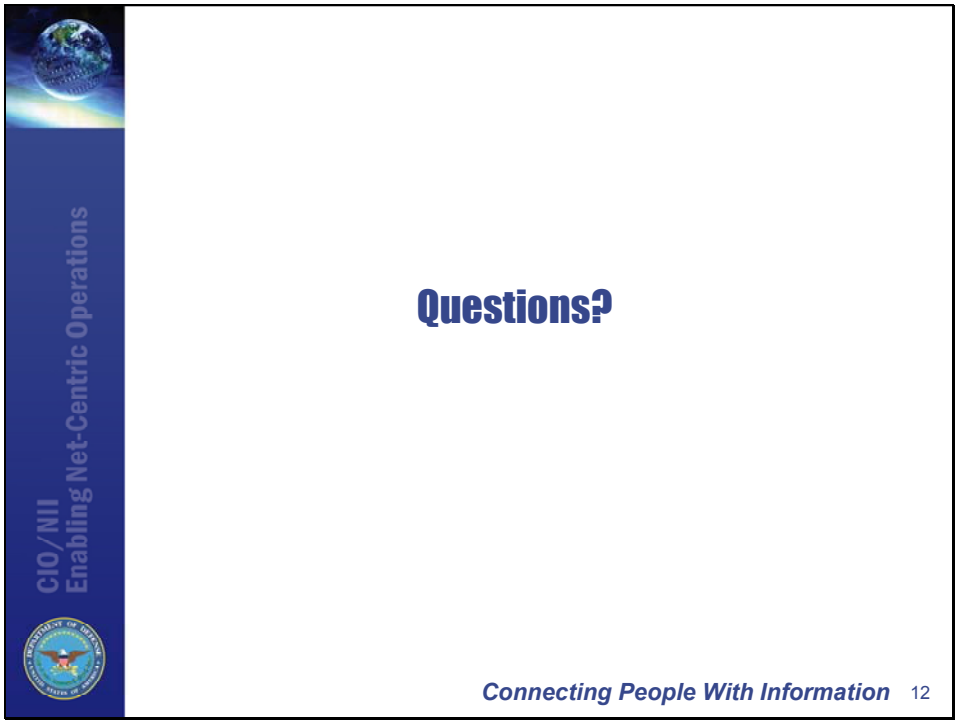
Where I need it

How I need it

Net-Centric Information Environment

Better Decisions Faster -- Decisive Actions Sooner

Connecting People With Information 11


CIO/NII
Enabling Net-Centric Operations
Questions?
Connecting People With Information
12

APPENDIX D

BREAKOUT SESSION SUMMARY SLIDES

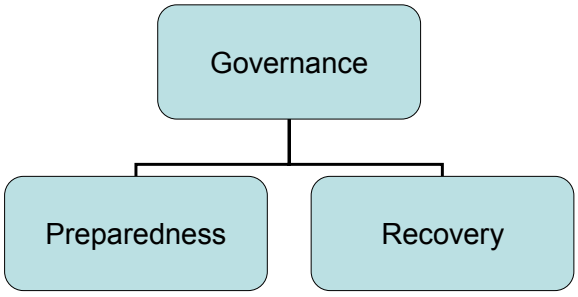
2006 RDX Workshop

International Internet Governance

Dr. Sy Goodman, Georgia Tech
Mr. Rod Wallace, Nortel

September 22, 2006

Governance Perspective



- Government, Nations
- Users
- Private Industry
- Technology Developers

R&D Areas

Issues Subject to Governance	Components	Baseline	Governance Gap Analysis	R&D Recommendations
Infrastructure Trust	• DNS • ENUM • Secure Routing • Party and Device Authentication • Web Services	• FIPS 201 • ICANN	• Lack of Federation Standards • Legitimacy and Mandate of Current Oversight Processes	• Governance When Components Merge • 3rd Party Evaluation of Current Oversight Processes and Recommendations
Misuse and Fairness*	• SPAM (as DOS) • Mal-code that abuses infrastructure • Directed Misuse • Protocol Misuse (BOTNET) • Abuse of Web Services	• NCRCG • IDWG • NVD • CVE/OVAL • Law Enforcement	• Other Critical Infrastructure Stakeholder Involvement • Incentives, Liabilities, and Misuse of Fairness	• Common Frameworks for Information Management • Common Assessment and Mitigation Tools
Enforcement and Resolution	• Real Time Information Sharing and Coordinated During Incident Response • Information Collection About Misuse and Fairness	• IWWG • Cyber Crime Treaty	• Lack of International Enforcement Body • Lack of Common Framework • ***Multi-lateral Mechanism to Develop and Implement Criteria for Horizontal Coordination***	• Preemptive Discovery • Develop of Criteria and Process to Achieve Multi-lateral Sharing and Response

* Excludes applications level abuses such as phishing
** Input in the matrix is representative examples

Policy Issues and Agenda for Action

Policy Issues for NSTAC Consideration:

- **Multi-lateralization of the national security component of network security policy while maintaining the integrity of network operations**
- **Maintenance of the balance in governance mechanisms between national interests (of/or articulated by Governments) and economic interests (of/or articulated by business) in operation and stewardship of critical ICT infrastructure**

Agenda for Action:

1. **Assessment/cataloguing of:**
   - **Existing rules, relationships (JCG, IWWG), analogues from other sectors (ICAO, IMO) of above**
   - **Baseline national governance mechanisms/policies in effect today for close allies**
   - **Current components that should come under governance mechanisms and evolution as we move to the NGN**
2. **Developing structure and membership of multi-lateral governance mechanisms to achieve the above**
3. **Investigate national security and economic security implications of technical and economic convergence**

2006 RDX Workshop

Global-Scale Identity Management Breakout Session

Reg Foulkes, CSC Canada
Tim Moses, Entrust

September 22, 2006

Current R&D Activities

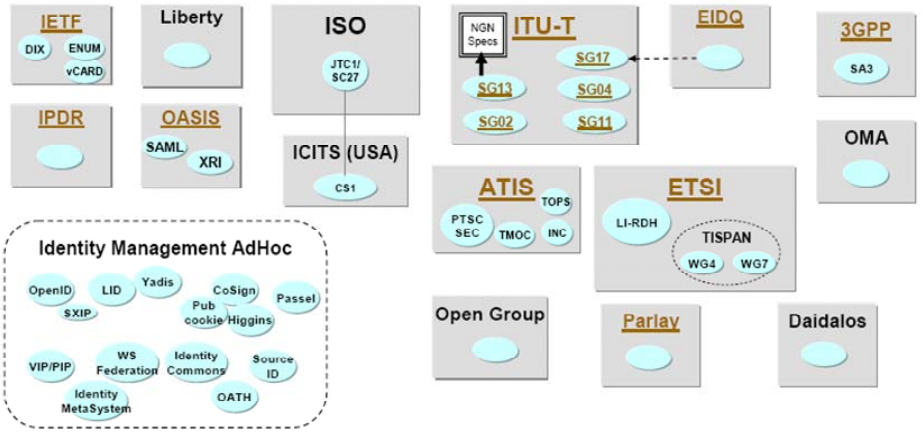
The following R&D activities are currently underway, which address *global-scale* identity management and serve to strengthen communications and cyber security:

Some have attempted to be global, but have only reached a regional level

- NIST / FIPS 201 (US)
- ISO SC29 & ITU-T SG13/17 (International)
- CardSpace (MSFT)
- ICAO (International)
- IdenTrust (Banking/International)
- Daidalos
- Liberty Alliance Project
- Global Grid Forum

* *This area deserves further attention*

Current Standards Activities



Key Research Areas

Specific research areas offer the most potential to improve identity management R&D in the future:

- Cross-border and cross-sector use-case scenarios and requirements
  - Privacy safeguards, failure use-cases, physical v. logical, disaster recovery, contingencies
- Platform-independent credentials (wireless devices, Internet cafes, etc.)
- Interoperability amongst IDM systems
  - Framework for cross-recognition of certification practices & data schema
  - Protocols, schemas, federation models, language support, etc.
- Assurance models –reliability metrics, additional safeguards
- Trust agreements
  - Acceptable error rates
- Cost models / business cases that accelerate global-scale deployment
  - Incremental benefit
- Glossary (e.g., semantics, vocabulary, common understanding of terms)

Potential Impediments

Impediments that might inhibit the development of identity management solutions that can be scaled to a global level:

- Sovereignty issues
- Funding considerations / resource allocation (how it's paid for)
- Infrastructure roll-out (e.g., cost, timeframe, incremental benefit)
- Diversity of platforms
- Privacy issues
- Issues of trust
- User acceptance
- Failure to agree on components of identity
- Lack of motivation to adopt global scale systems (e.g., tax breaks, regulatory mandates)

Policy Issues

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

- Ownership of identity (Fair Information Practices)
  - Transferring credentials across domains
  - Sovereignty – achieving multi-lateral agreements
- Agreed upon minimum set of attributes that constitute an identity
  - Application dependent
- Guarantees for privacy in national security and emergency preparedness applications
  - Understanding of information boundaries and privacy implications
  - Mandatory or voluntary enrolment
- Conditions for anonymity and pseudonymity including operations security
- Risk appetite (false positives and negative rates)
  - Graduated levels of assurance
- Commercial issues (trade implications, competitiveness, regulatory mandates)
- Legal and liability considerations

Roles & Responsibilities

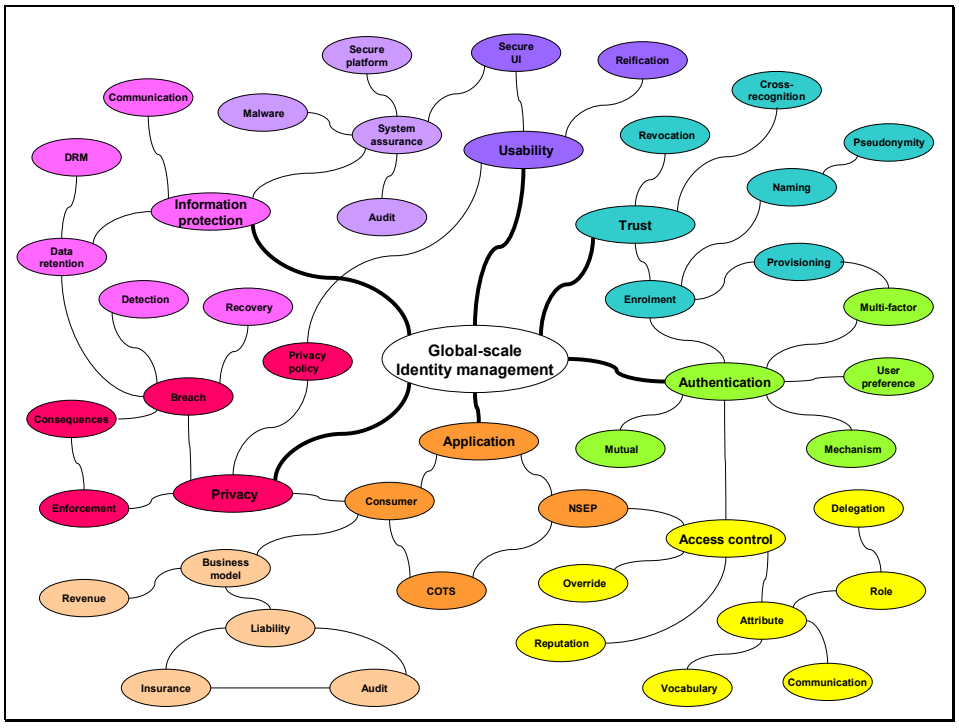
Industry, academia, and Government all have unique roles and responsibilities in funding and advancing R&D for identity management:

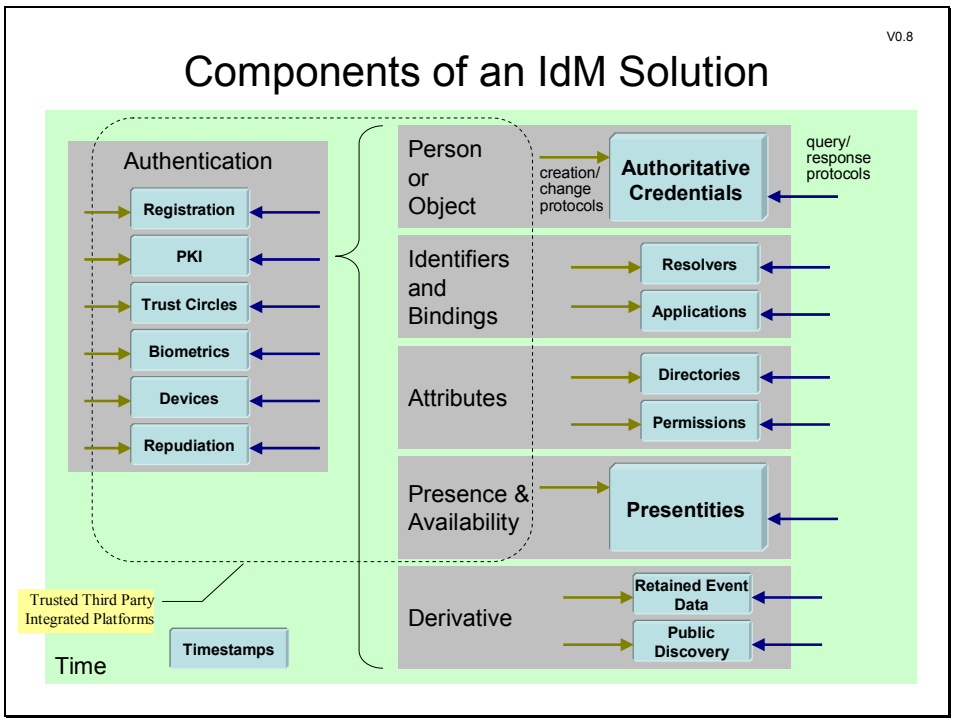
Academia	• Vulnerability Research • Glossary
Industry	• Technology solutions • IDM in the workplace
Government (Roles for agencies responsible for regulatory, justice, and infrastructure protection)	• Incentive plan for enhanced infrastructure and security • Scenario development • Interagency collaboration
Others?	• Standards bodies • Centers of Excellence

Agenda for Action

An "Agenda for Action: International Collaboration for Identity Management" should —

- Develop cross-border and cross-sector use-case scenarios and requirements
- Define ownership of identity (including transferring credentials, sovereignty)
- Identify Centers of Excellence for identity management R&D to encourage collaboration, maintain repository of ongoing initiatives, and identify promising technologies
- Agreement on models for assurance, risk and trust
- Promote education and awareness
- Glossary (e.g., semantics, vocabulary, common understanding of terms)
- Adapt policy for privacy and resolve legal and liability issues
- Advance supporting and interoperable infrastructure


Secure platform
Secure UI
Reification
Communication
Malware
System assurance
Usability
Cross-recognition
Revocation
Pseudonymity
DRM
Naming
Information protection
Audit
Trust
Data retention
Provisioning
Detection
Recovery
Enrolment
Multi-factor
Privacy policy
Global-scale Identity management
Authentication
User preference
Breach
Consequences
Application
Mutual
Mechanism
Privacy
Consumer
NSEP
Delegation
Enforcement
Access control
Business model
Override
Role
Revenue
COTS
Attribute
Liability
Reputation
Insurance
Audit
Vocabulary
Communication


V0.8
Components of an IdM Solution
Authentication
Registration
PKI
Trust Circles
Biometrics
Devices
Repudiation
Person or Object
creation/ change protocols
Authoritative Credentials
query/ response protocols
Identifiers and Bindings
Resolvers
Applications
Attributes
Directories
Permissions
Presence & Availability
Presentities
Derivative
Retained Event Data
Public Discovery
Trusted Third Party Integrated Platforms
Timestamps
Time

2006 RDX Workshop

Collaborative Mechanisms for Network Security Protocol Research and Development Breakout Session

Mr. Jim Brookes
Mr. Marc Sachs

September 22, 2006

Goals of the R&D Consortium

Create an International R&D Consortium which:

- Enables collaboration on big ticket security research topics
  - ➢Leverages existing funding sources to address research priorities
- Addresses the compelling network security risks to public safety issues and economic sustainability
- Identifies and works on the highest priority issues as noted by partners
- Creates a trusted collaborative environment between governments, industry, and academia

Current R&D Collaboration Mechanisms

Numerous examples of collaboration mechanisms exist for shaping future mechanisms to address cyber security concerns:

- PREDICT
- DETER
- Planet Lab
- Internet 2*
- Cylab*
- Caida
- Network Centre of Excellence
- The Technical Cooperation Panel
- European Commission Frameworks Programs*
- Public Security Technology Program
- BITS
- National Science Foundation's GENI
- Research Triangle Park
- Logic
- I3P
- Technical Support Working Group
- In-Q-tel
- SEMATECH
- IEEE
- Technology incubators
- Network Security Information Exchange

Collaborative Models

- Grant model
- Membership model
- CRADA model
- Volunteer model
- Memoranda of Understanding
- Bi and Multi-laterals
- Treaties
- Economic incentive model
- Government only
- Industry only

Strengths of Existing Collaboration Models

Several existing mechanisms possess strengths that should be considered:

- Good approach to industry involvement and funding - Cylab
- Requires involvement of multiple countries - European Commission Frameworks Programs
- Framework for future networks - Internet 2

Attributes for Collaboration

Specific attributes of a proposed collaboration model include:

- An international scope
- Support for networking and collaboration of all participants and advocacy for research
- Sustainability in the long term
- Access to real industry data by university researchers
- Safe harbor language (liability, background check laws) and relief from International Trade and Arms Regulations
- Community (government, industry, academia) endorsement
- The development of an intellectual property regime
- The provision of a funding model (supported by government and industry which provide funding and personnel; recognizes size of partner)
- The provision of a technology transition model (licensing)
- Clear guidelines for publication of results
- Trust and openness
- Meaningful output for participants

Potential Impediments

Impediments that might inhibit collaborative mechanisms for enhancing R&D:

- Intellectual property, copyright, and patent restrictions
- Export control
- Citizenship of researchers
- How to protect member data
- International Trade and Arms Regulations
- Lack of community endorsement
- Requiring clearances for students
- Ethics standards for research with humans
- Unclear equation for determining benefits based on contribution
- Commitment to sustain research
- Restrictive data markings

Why the Market Does Not Work

There is a market failure to address these compelling research issues because:

- The marketplace relies on government to address public safety, economic viability, and social issues caused by threats to the Internet and Internet technologies
- There is too much uncertainty on the risks we are facing
- Market does not effectively address public infrastructure problems
- "Magic bullet" solutions have the potential to drain important resources from longer term approaches that may be more effective in the long-term
- Scope of activity broader than any single participant
- No alignment between those who incur costs and those who benefit

Research Agenda

Top 5 priorities include:

1. Wide scale situational awareness for attack prediction and detection
2. More resilient and secure protocols
3. Global scale authentication and identity management
4. Secure and scaleable routing infrastructure
5. Security metrics

Research Agenda (continued)

Other priorities include:

1. Dynamic risk environment
2. Deployment of R&D solutions
3. Strongly authenticated network control plane
4. End user and developer appreciation for security concerns
5. Enterprise rights management
6. Assured end to end communications in a deregulated carrier environment
7. Improved and implemented software and system engineering methodologies
8. Scaleable naming system
9. Collaborative traceback of attackers
10. Support for lawful intercept
11. Authorization and policy enforcement on a wide scale
12. Information based policy enforcement (dynamic)

Policy Issues

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

- Legal concerns associated with sharing intellectual capital amongst member entities
  - Anti-trust
  - Freedom of information
- Governmental policy for sharing information across borders
- Privacy of individual citizens
- Membership eligibility criteria
- Appropriate role for governments
- Commitment to support and implement agreed upon solutions

Roles & Responsibilities

Industry, academia, and Government all have roles and responsibilities in communications and cyber security R&D collaboration:

Academia	• Provide university researchers to participate in consortium that facilitates global research • Help set research agenda • Link with other research programs
Industry	• Provide funding support • Help set research priorities • Participate in consortium that facilitates global research • Provide metrics
Government	• Provide funding support • Help set research priorities • Participate in consortium that facilitates global research • International government-to-government coordination • Link with other related-government programs • Enact appropriate laws or regulations that support collaborative research • Provide neutrality (venues/leadership)
End Users	• Help set research priorities and requirements • Provide context

Agenda for Action

The next steps to establish this international collaboration are —

- Enlist an inspiring champion to launch the initiative and:
  - ➢Identify and communicate with key stakeholder groups
  - ➢Define business plan
  - ➢Develop funding proposal
  - ➢Define and establish international collaboration framework
  - ➢Engage international partners
- Put in place a governance model for the collaborative effort
- Develop a value proposition for each group of participants

2006 RDX Workshop

Cross-Border & Cross-Sector Challenges Breakout Session

Mr. Stuart Brindley, Independent Electricity System Operator
Dr. Jack Oslund, George Washington University

September 22, 2006

Current R&D Activities

The following R&D activities are currently underway, which address cross-border and cross-sector challenges and serve to strengthen communications and cyber security:

- Existing "Roadmap to Secure Control Systems in the Energy Sector"
  - Developed by: Private Sector, DOE, NRCan, DHS, PSEPC
- The Technical Cooperation Panel (TTCP)
  - Developed by: Five allied nations
- Linking Oil Gas Industry Infrastructure Cyber Security (LOGIIC)
- Secure Wireless Communications
- DETER Testbed
- Common cyber security approach across sectors
  - Developed by: SANS Institute, DOE
  - Common Criteria

Potential Impediments

Impediments that might inhibit collaborative R&D to advance cross-sector and cross-border collaboration in the future are:

- Current collaboration is limited and localized; it should be combined and leveraged across sectors and borders
  - Initiatives are "stove-piped" or "silo-ed"; need to find common threads
  - Leadership is needed to coordinate efforts
- Secure mechanisms for information sharing across borders have not been exercised or tested
  - Need to probe deeper on interdependencies
  - Establish the "ground truth" beyond modeling efforts to date
- Sector-specific jargon exists between sectors
- Proprietary considerations can be counter-productive to information sharing
- Contrasting R&D programs between the five allied nations and European Union
- Cost and scheduling challenges in government and private sector R&D
- Managing for very low probability events

R&D Policy Issues

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

- Limited willingness or ability to share classified or sensitive information intra-sector, cross-sector, and cross-border
  - Need a process for engaging people
  - "Need to share" rather than "need to know"
- Barriers to establishing new partnerships and broadening existing partnerships
  - Tendency to favor "products" over "value of partnerships"
  - Lack of information and common goals/priorities
  - Cross-sector and cross-border
- Failure to anticipate generational changes in how technology will be used
- Education – development / implementation life cycle is not in place
  - Lack of eligible potential employees for NS/EP work
- New trust structures for new online tools

Agenda for Action

An "Agenda for Action: International Collaboration for Cyber Security and Assured Communications" should —

- Create incentives for private sector to include NS/EP requirements as part of product development
- Prepare an inventory of existing R&D initiatives; identify priorities
  - Cross-sector and cross-border
  - Cyber security and information assurance
- Move beyond narrow bilaterals between governments
  - Greatly enhance private cross-sector participation
  - Build on five allied nations with common interests and goals
- Enhance R&D to probe and establish "ground truth", e.g.,
  - Interdependency modeling efforts
  - More substantive exercises
- Establish priorities for restoration and managing reduced capacity
  - "Who's on first?"

An Example of Success:

Leverage the "Roadmap to Secure Control Systems in the Energy Sector" and promote international collaboration

- *Adapt to telecommunications sector*
- *Broaden international collaboration*

2006 RDX Workshop

Wireless and Mobile Ad Hoc Network Applications

Facilitators:
Dr. Julie Lefebvre, DRDC Ottawa
Mr. Mike Alagna, Motorola

September 22, 2006

Breakout Session Team Members

- Wide cross-section of participants:
  - Industry (service providers, equipment vendors, infrastructure owners)
  - Government (U.S. and Canada)
  - Academia
- Wide variety of perspectives :
  - R&D Practitioners
  - Technology Implementers
  - User Community (e.g., National Security/Emergency Preparedness)

… representative of R&D Exchange participants at large

Major Discussion Themes

- Basic discussion on dimensions of issue/scope of problem – Why MANET?
  - Effective when infrastructure is lost
  - Robust connectivity (e.g., mitigate single points of failure)
  - Flexibility
  - Fault tolerance (self healing)
- Application to Emergency Response/Military/Public Safety communities:
  - Lessons Learned from Hurricane Katrina Response
  - Operability versus Interoperability
  - Scenario-specific security requirements (temporary vs. permanent app)
- Identification of Current R&D Activities/Academic Focus Areas
- Transition of current security implementations into MANET environment
- Impediments to technology adoption and further R&D
- Identification of Priorities

Current R&D Activities

The following R&D activities are currently underway, which address wireless ad hoc networks and serve to strengthen communications and cyber security:

- EU Project: WIDENS
- NIST: MANET & Sensor Network Security
- Distributed test Bed for 1st Responders
- Project Mesa
- CERDEC: Multi-Dimensional Assured, Robust Communications on-the-move Network-I (MARCOM-i) STO Program
- DARPA
- DRDC
- Strong Authentication with no central trusted authority
- Secure Routing
- Lack of Capacity
- Interoperability
- Functionality
- Intrusion Detection
- Location-based Services
- Sensors/logistics

Key Technology Areas

- Global Deployments/Registry*
- Group Key for interoperability, dynamic changes and scale*
- Test Bed/Standards/ Certification/Requirements*
- Mobility/Usability*
  - authentication/bio metric/voice*
  - authorization
  - audit
  - QoS +Security (priority)
  - intrusion detection/protection
  - DOS/Protection
  - Hybrid Nets
- 802.11 i/n automated security (and others)
- Customized simple chip/low cost
- Sensors+RFID
- Cognitive radio/SDR/Spectrum
- Privacy Issues
- Policy-based Management
- Human Factors/Interface
- Location-based service*
- Development and Sharing of Best Practices
- IP/IPv6
- IBE
- Discovery mode strategies

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

Potential Challenges & Impediments

• "No killer app in commercial space" - Lack of business case/ lack of paying "customer" for non-military use

• Lack of Vision/CONOPS for MANET deployments to justify R&D focus (e.g., separate visions addressing military and civilian space)

• Cross border coordination on ongoing R&D to leverage available R&D dollars

• Transition Issues from current environment to a secure MANET architecture

- Human/Culture issues (in an operational environment)
- Acceptance of multinational standards
- Clearance level / foreign disclosure allowing info sharing
- Lack of Forums to socialize the need
- Export control/IPR, liability, privacy issues
- Lack of suitable test-beds for security and accreditation

• Not enough being done: education training, standards/standardized, interoperability, bring down cost of security, testing cases involving international collaboration

Identified Priorities

• **Human Factors: Culture, Governance, Jurisdiction, Trust – in an operational environment**

Technology Investment Areas: Identity Management for Global, Dynamic, Technology-agnostic, Hierarchical, Meshed Networks. Technologies that meet diverse requirements of/take into account/enable communities of interest. Include culture/human factors in tech development, planning, exercises.

• **Open doors to foster collaboration, innovation, information sharing, R&D Sharing and Coordination, Standards and Policy Development**

Investment Area: Applications addressing communities of interest; cost of collaboration; Inventory of current state, Increased flexibility with filtering monitoring; increased trials, info sharing forums; adequate controls (trust)

Identified Priorities (continued)

• **Hybrid networks for "Seamless Mobility"**

Investment Areas: Operability/Interoperability/Spectrum, and Assured Communications.

- Leverage military MANET R&D for commercial application
- Analyze transition/migration strategies from current security implementations to next generation MANET
- Supporting NS/EP assured communications through next generation MANET implementations, including Identity Management and Security QoS
- MANET as an enabler of "Seamless Mobility" – the killer app?
- MANET applicability to resolve spectrum management/interoperability issues?

APPENDIX E

SPEAKER AND FACILITATOR BIOGRAPHIES

Speaker and Facilitator Biographies

F. Duane Ackerman is Chairman and Chief Executive Officer (CEO) of Atlanta-based BellSouth Corporation. A native of Plant City, Florida, Mr. Ackerman holds a bachelor's degree in physics and master's degree from Rollins College in Winter Park, Florida, and a master's degree in business from the Massachusetts Institute of Technology.

Mr. Ackerman began his communications career in 1964, and has served in numerous capacities with BellSouth. Mr. Ackerman was named President and CEO of BellSouth Telecommunications, BellSouth's local telephone service unit and largest subsidiary, in November 1992. He was promoted to Vice Chairman and Chief Operating Officer of the parent company, BellSouth Corporation, on January 1, 1995, and was elevated to the position of President and CEO of BellSouth on January 1, 1997. On January 1, 1998, Mr. Ackerman was appointed Chairman and CEO of BellSouth.

In addition to serving as a director of BellSouth Corporation, Mr. Ackerman is also a member of the board of The Allstate Corporation. Mr. Ackerman is the immediate past Chairman of the National Council on Competitiveness, Chairman of the NSTAC, member of the Homeland Security Advisory Council, member of the President's Council of Advisors on Science and Technology, a trustee of Rollins College and a former member of the Board of Governors for the Society of Sloan Fellows of the Massachusetts Institute of Technology.

Michael Alagna joined Motorola in 1985 as a systems engineer/engineering manager and supervised systems engineering group in support of design & implementation, for United States (U.S.) Government solicitations. Over the last 20 years, he has assumed increasing management responsibility in customer facing roles including responsibility for worldwide international sales, coordinated global marketing efforts and as a certified program officer, was responsible for all aspects of key international projects. In a business development role, he managed the Iridium Satellite go to market strategy and established a worldwide distribution organization including marketing, lead generation & tracking, training, order fulfillment and customer relations.

Mr. Alagna has managed Motorola's strategic planning for U.S. Federal Government, DOD and international wireless communication programs. As such, he has developed an extensive understanding of the Federal Government's wireless communication priorities and needs. He also served as Vice President of Motorola's Integrated Solutions Group, providing him a strong background in critical large system integration transition challenges. Most recently he is focused upon strategic marketing initiatives and policy. Mr. Alagna received a Bachelor's Degree from University of Maryland, and a Master's Degree in Business Administration from Michigan University. He is a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee.

Anthony Ashley began his career as a Defence Scientist at the Defence Research Establishment Atlantic in Dartmouth Nova Scotia, Canada. During the 1980s and 1990s, he led programs that developed and demonstrated concepts that provide the core functionality of sonar systems that are now in use by the Canadian Forces, Belgium, and Portugal.

In 2000, Dr. Ashley became Director of Science and Technology (S&T) Maritime in Ottawa where he was responsible for directing and coordinating the Maritime Research and Development program. As Chief Scientist at Defense Research and Development Canada (DRDC) Ottawa he oversaw the development of the scientific capacity of the laboratory in a number of diverse fields including radar, radio frequency, electronic warfare, navigation warfare, synthetic environments, network information operations, intelligence, surveillance and reconnaissance systems, and radiation detection.

In his current role as Director General of the Centre for Security Science at DRDC, he and his team are developing a S&T program for public safety and national security. Dr. Ashley has a Bachelor of Science, a Master of Science, and PhD in Electrical Engineering from the University of Manitoba.

Stuart Brindley is the manager of Training & Emergency Preparedness with the Independent Electricity System Operator (IESO) in Ontario, Canada. The IESO is responsible for operating and regulating Ontario's wholesale electricity system and the wholesale electricity marketplace—linking buyers and sellers while directing the flow of electricity on Ontario's transmission system from generators and suppliers to local distribution companies and wholesale buyers.

Mr. Brindley is Chairman of the North American Electric Reliability Council's Critical Infrastructure Protection Committee, which works with industry and Government sectors to help protect the electricity infrastructure from cyber and physical attacks and respond to emergencies.

Mr. Brindley also serves as Chairman of the Partnership for Critical Infrastructure Security, which represents all critical infrastructures in their collaboration with the United States Department of Homeland Security.

Jim Brookes is the Chief Operating Officer for Mathematics of Information Technology and Complex Systems (MITACS), a Network of Centres of Excellence (NCE) for the mathematical sciences. MITACS focuses on developing mathematical solutions addressing issues in key sectors of the Nation's economy, including information security. Mr. Brookes previously worked in the telecommunications sector with BC Tel, Stentor and TELUS. He held a variety of senior positions in Business Development, Marketing, and General Management. Mr. Brookes was Vice-President of Local Services at BC Tel/TELUS where he grew a $2B market and was also Vice-President of Business Transformation at TELUS. He has testified as an expert witness at several landmark regulatory proceedings.

Mr. Brookes has a Bachelor's Degree and Master's Degree in Economics from Simon Fraser University. He is a member of the Board of Directors for VanDusen Botanical Gardens as well as two high technology start-up companies.

Guy Copeland is Vice President, Information Infrastructure Advisory Programs, with Computer Sciences Corporation (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 NSTAC,. He currently chairs the NSTAC's RDTF, which organized the R&D Exchange Workshop in Ottawa, Canada.

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 IT ISAC where he recently completed a term as President. Mr. Copeland was elected, in January 2006, by the membership of the newly created Information Technology Sector Coordinating Council (IT SCC) to be its first Chairman. Within the Information Technology 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 U.S. 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.

Peter Fonash was formally assigned as the Deputy Manager and Director of the National Communications System (NCS) on April 21, 2005, after serving 9 months as the Acting Deputy Manager. From 1998 until July 2004, Dr. Fonash served as the Chief of the NCS Technology and Programs Division, managing priority services technology development, network modeling and analysis, specialized telecommunications research and development, and priority services standards. He also supervised the acquisition of priority communications services in the Public Switched Network through the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs.

Prior to arriving at the NCS, Dr. Fonash accelerated the Electronic Commerce program for the DOD Chief Information Officer and served as the Chief, Joint Combat Support Applications Division, providing technical integration services to the functional communities and guiding functional applications' compliance with the standard common operational environment.

Working for the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence from 1994 to 1996, Dr. Fonash was responsible for policy and program oversight of the Defense Information Infrastructure, and served as Chairman, Office of the Secretary of Defense Information Technology Architecture Council. From 1986 to 1994 Dr. Fonash held various management and technical positions in the Defense Information Systems Agency (DISA), including Director of Technology (Center for Information Management) and Chief of the Advanced Technology Office.

Prior to working for DISA, Dr. Fonash was assigned to the position of Army Deputy Director, Ada Joint Program Office from 1981 to 1984. From 1984 to 1986 he was the project manager for the Software Technology for Adaptable Reliable Systems methodology project under the Army Materiel Command.

Before entering Government service, Dr. Fonash was responsible for systems engineering of international switching and all signaling systems in Eastern Region of AT&T Long Lines. He was also a Deputy Group Leader for the Planning Research Corporation, managing and marketing engineering services to clients. As a Senior Financial Analyst and Systems Analyst for the Burroughs Corporation (Unisys), he was responsible for development, modifications and maintenance of accounts payable, production planning, and financial information systems. In this position he prepared forecasts and budgets for the United States division of the company.

Dr. Fonash has a Bachelor of Science and a Master of Science in Electrical Engineering from the University of Pennsylvania, a Master of Business Administration from the University of Pennsylvania Wharton School, and a PhD in Information Technology from George Mason University, School of Information Technology and Engineering.

Reg Foulkes is a strategic and technical executive with 23 years of diversified leadership and managerial experience, encompassing state-of-the-art information technology, application architecture and management, all facets of data security, directory management, systems and process architecture, and software engineering.

Mr. Foulkes is the Director and Chief Technology Officer for Global Security Solutions within CSC Canada. He focuses on evaluating emerging and future technology as well as recommending appropriate architectures, technologies, key partnerships, process, or policy changes that would enable organizations to meet key business goals, new and existing legislation or audit procedures in a global environment. Mr. Foulkes is based in Ottawa, Ontario, Canada.

Seymour Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of the Center for International Strategy, Technology, and Policy and Co-Director of the Georgia Tech Information Security Center.

Dr. Goodman studies international developments in the information technologies and related public policy issues. In this capacity, he has published well over 150 articles and served on many Government and industry advisory and study committees. He has been the International Perspectives editor for the Communications of the Association for Computing Machinery for the last sixteen years. Dr. Goodman is currently serving as Chair of the Committee on Improving Cyber Security Research in the United States, National Research Council, Computer Science and Telecommunications Board, National Academies of Science and Engineering.

Immediately before coming to Georgia Tech, Dr. Goodman was the director of the Consortium for Research in Information Security and Policy, jointly with the Center for International Security and Cooperation and the School of Engineering, Stanford University. He has held appointments at the University of Virginia (Applied Mathematics, Computer Science, Soviet and East European Studies), The University of Chicago (Economics), Princeton University (The Woodrow Wilson School of Public and International Affairs, Mathematics), and the University of Arizona (Management Information Systems, Middle Eastern Studies). Dr. Goodman was an undergraduate at Columbia University, and obtained his PhD from the California Institute of Technology.

John Grimes was nominated by President Bush on June 17, 2005, and sworn in as the Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer, Department of Defense (DOD), on November 14, 2005. Mr. Grimes has extensive technical and policy experience in telecommunications, information systems, and the command and control fields.

His public service includes five years on the White House National Security Council Staff as Director for National Security Telecommunications Policy, Director of Defense Command, Control and Communications Programs, and Senior Director White House Situation Support Staff from 1984 to 1990. Mr. Grimes served as Deputy Assistant Secretary of Defense for Command, Control and Communications and was the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures from 1990 to 1994. As a member of the DOD senior executive service, he held senior technical and staff positions with the National Communications System, Defense Communications Agency (predecessor to DISA), and the U.S. Army Communications Command following his military service in the U.S. Air Force.

Mr. Grimes joined Raytheon Company in 1994 where he served as Vice President of Intelligence and Information Systems, Washington Operations, prior to retiring in November 2005. Mr. Grimes has served on four Defense Science Board Task Forces. He was a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee.

A native of Fredrick, Maryland, Mr. Grimes is a graduate of the University of Arizona and also holds a Master of Science Degree from Shippensburg University in Pennsylvania. He is a graduate of the U.S. Army War College, Carlisle Barracks, Pennsylvania; the Federal Executive Institute, Charlottesville, Virginia; and Harvard University's National and International Security Policy Program. He is the recipient of the American Institute of Aeronautics and Astronautics' Command, Control, Communications and Intelligence (C3I) Award among other public, military and Federal civil service awards to include two Presidential Rank awards.

Priscilla Guthrie is Deputy Assistant Secretary of Defense, Networks and Information Integration, and Deputy Chief Information Officer at the DOD. Prior to her post at the Pentagon, Ms. Guthrie was vice president of e-Business at TRW Inc. in Washington, Michigan. She has more than three decades of management experience in business enterprise systems, information technology infrastructure and telecommunications systems.

Ms. Guthrie began her career at TRW in 1972, providing technical support on signal processing and modeling tasks. From 1974 through 1978, she worked on signal processing development efforts. In 1978 she was named head of a systems engineering section, supervising systems engineering and integration efforts for several large projects.

Her tenure at TRW included serving as manager of the Systems Software Development Laboratory, director of Navy Systems Development, director of North American Operations Automotive Aftermarket, and vice president and general manager of the Commercial Market Area for TRW's Systems and Information Technology Group.

Ms. Guthrie earned a Bachelor of Science Degree in Electrical Engineering from Pennsylvania State University and a Master's Degree in Business Administration from Marymount University. She remains highly involved with Penn State University. She was a board member of the Penn State Engineering Society and the College of Engineering's Leonhard Center Advisory Board and was a past chair of the Women in Engineering Program Advisory Board. In May 2000, Ms. Guthrie presented the commencement address at the College of Engineering's spring graduation ceremony. She received the Outstanding Engineering Alumna Award in 2001, the highest honor bestowed by the College of Engineering. Ms. Guthrie was also named an Alumni Fellow by the University in 2003.

She serves on the boards of the Northern Virginia Technology Council and the Fairfax Symphony Orchestra.

Annabelle Lee is the Director, Security Standards, Best Practices and R&D Requirements in the National Cyber Security Division of the Department of Homeland Security (DHS). Her responsibilities include engaging with other Government agencies, academia, and industry for the development of cyber security R&D requirements, metrics, and standards. Dr. Lee also co-chairs the Cyber Security and Information Assurance Interagency Working Group with the Office of Science and Technology Policy. This working group recently published the Federal Plan for Cyber Security and Information Assurance Research and Development that provides a blueprint for coordination of Federal R&D across agencies. The Plan's findings and recommendations address R&D priority-setting, coordination, fundamental R&D, emerging technologies, road mapping, and metrics. The working group is coordinating the cyber security R&D priorities and roadmap efforts with international partners. The objective is to leverage the knowledge and resources of the various organizations that are defining cyber security R&D requirements globally and implementing research programs.

Dr. Lee's experience comprises over 30 years of technical experience in IT system design and implementation and almost 20 years of IT security specification development and testing. Over her career she has authored or co-authored many documents on IT security, cryptography, and

testing. She began her career in private industry concentrating on software testing and quality assurance.

Prior to her current position, Dr. Lee was the Acting Director for the Cyber Security Portfolio in the DHS Science and Technology Directorate. Her responsibilities included leading an Integrated Product Team that developed the Cyber Security R&D Portfolio and interfacing with other organizations within DHS that are the internal customers for the cyber security R&D programs.

Prior to DHS, Dr. Lee was a Senior Security Engineer at the Computer Security Division in the National Institute of Standards and Technology. Dr. Lee participated as a member of the team that developed a family of Certification and Accreditation documents. Previously, she was the Director of the Cryptographic Module Validation Program. Dr. Lee was the technical lead for the development of Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*, and initiated the submission of the standard to International Organization for Standardization.

Julie Lefebvre received her PhD degree in theoretical physics from McMaster University in 1995. She joined DRDC – Ottawa in 1999 and has since been conducting research in computer network security.

Her current research interests are in computer network defence situational awareness, coalition information assurance and information operations. Since 2005, Dr. Lefebvre has been leading the Network Information Operations Section at DRDC Ottawa, which is responsible for computer network security research and development for the Department of National Defence.

Doug Maughan is a Program Manager in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Department of Homeland Security S&T Directorate. Dr. Maughan directs the Cyber Security Research and Development activities at HSARPA. 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 the National Security Agency as a senior computer scientist and led several research teams performing network security research.

Dr. Maughan received Bachelors' Degrees 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.

Tim Moses is the Senior Director of the Advanced Security Technology group at Entrust, where he is responsible for Entrust's research and standards activities. He holds Bachelor's of Science and PhD degrees in electronic engineering and has over 30 years experience in industry. He has worked in the field of information security, in both product design and consulting capacities, for the past twenty years.

Dr. Moses' current research interests include enhancing the trustworthiness of the Secure Sockets Layer, for which he is the chair of the Certificate Authorities/Browser Forum, and multiauthentication techniques, for which he is defining a framework architecture for integrating authentication mechanisms into on-line business processes. Recently, he was the editor of the Extensible Access Control Markup Language policy language standard for access control. Additionally, he has been actively involved in the development of security negotiation techniques for service-oriented architecture.

The team under Dr. Moses' direction participates in the leading industry forums where standards for interoperability of large-scale identity, authorization, security and privacy management systems are defined. These include the Organization for the Advancement of Structured Information Standards, Internet Engineering Task Force, American National Standards Institute, Initiative for Open Authentication and others.

Dr. Jack Oslund, presently an adjunct professor, developed, coordinated and lectured in the Graduate Certificate Program in "Telecommunication and National Security" at the George Washington University, and was selected to be a Senior Fellow at the University's Homeland Security Policy Institute. He retired in 2000 from the former Comsat Corporation where he served in a variety of senior management positions involving United States signatory roles in Intelsat and Inmarsat, and was Director of Corporate Regulatory Relations.

During the latter part of his career at Comsat, Dr. Oslund was selected for five terms as Chairman of the Legislative and Regulatory Task Force of NSTAC and has participated on NSTAC task forces ever since. He has testified on Critical Infrastructure Protection issues before Congress, co-edited a book—*Communications Satellites: Global Change Agents* (2004)—and contributed chapters and/or articles to books, Congressional reports, journals and trade publications.

Immediately prior to joining Comsat, Dr. Oslund was an International Staff Officer in the White House Office of Telecommunications Policy; he also was a faculty member at the Joint Military Intelligence College (formerly the Defense Intelligence College), and an officer in the United States Marine Corps.

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 Telecommunications Union (ITU), the Organization of American States, and with the U.S. 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 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 U.S., 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 PhD 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.

John Roese, as Nortel's Chief Technology Officer (CTO), is responsible for leading the overall R&D strategy and execution, directing future research across all product portfolios. He also works closely with the Chief Strategy Officer on emerging technologies, market opportunities, and strategic partnerships.

Prior to joining Nortel, Mr. Roese was vice president and CTO for networking technologies at Broadcom Corporation, a semiconductor company, where he was responsible for the long-term architecture and technical strategy for networking technologies. These technologies included optical, power over Ethernet, switching, routing, security, broadband processors, fabrics and software elements.

Before joining Broadcom, Mr. Roese served as CTO at Enterasys Networks which specializes in network security for enterprise. At Enterasys, Mr. Roese oversaw the development of the company's technology architectures including comprehensive quality of service, security, management and transport services. Additionally, he was responsible for the company's initiatives in the Internet2/Next Generation Internet effort and headed the worldwide marketing and IT organizations. Previous to Enterasys, Mr. Roese was the CTO of Cabletron Systems where he was one of the key architects of Cabletron's SecureFast Switching.

Mr. Roese is actively involved in the IEEE and Internet Engineering Task Force, as well as other standards bodies, co-authoring a number of IEEE standards and related documents. In 1998, Mr. Roese published Switched Local Area Networks: Implementation, Operation, Maintenance (McGraw Hill). He is the named inventor on 16 granted and pending patents in areas of policy-based networking, location-based networking, routing, switching, and network management.

Mr. Roese holds a Bachelor of Science in Electrical Engineering from the University of New Hampshire. He is based at Nortel's R&D headquarters in Ottawa, Ontario, Canada.

Marcus Sachs is a deputy director of SRI International's Computer Science Laboratory where he supports the Washington, D.C. operations of the Cyber Security Research and Development Center. The Center is the primary vehicle through which HSARPA Cyber Security Research and Development programs are executed.

Mr. Sachs' professional experience includes a 20 year military career as an officer in the United States Army followed by two years of federal civilian service as a Presidential appointee at the White House and an initial member of the U.S. Department of Homeland Security. Mr. Sachs holds a Master's Degree in Computer Science from James Madison University, a Master's Degree in Science and Technology Commercialization from the University of Texas, and a Bachelor's Degree in Civil Engineering from the Georgia Institute of Technology. Mr. Sachs volunteers as the director of the SANS Internet Storm Center, serves on several industry advisory boards, and is frequently quoted by the media as a cyber security expert.

Patricia Sauvé-McCuan, as the Assistant Deputy Minister, Information Management, is responsible for leading the planning, delivery, and operation of information management assets and associated information technologies to support the missions, operations, and administration of the Department of National Defence (DND) and the Canadian Forces. The Information Management Group is organized into four Divisions, one Formation, a number of field units, and the Communication Reserve. The Divisions are located in Ottawa, while the field units are located across the country.

Ms. Sauvé-McCuan joined the DND in September 2004 as Director General, Information Management Project Delivery before being appointed Acting Assistant Deputy Minister, Information Management, in August 2005, and ultimately Assistant Deputy Minister, Information Management, in March 2006.

Ms. Sauvé-McCuan's career brings together a blend of private and public sector experiences, with expertise in operational, financial, and information management. Before joining the DND, Ms. Sauvé-McCuan held a number of financial and Information Management positions, most notably as Senior Vice-President for CogniCase Ottawa Ltd and Vice-President with R3D Information and Technology, an organization specializing in Project, Program, and Business Program Management Services.

Bob Stephan (U.S. Air Force, retired) was appointed to serve as the Assistant Secretary of Homeland Security for Infrastructure Protection, Preparedness Directorate, United States Department of Homeland Security, in April 2005. In this capacity, he leads the coordinated national effort to reduce the risk to our critical infrastructures and key resources posed by acts of terrorism, while increasing the Nation's preparedness capability focusing on critical infrastructure protection.

His prior experience as Senior Director for Critical Infrastructure Protection in the Executive Office of the President (EOP) makes him a well qualified choice for the Assistant Secretary position. During his tenure with the EOP, his duties included developing and coordinating interagency policy and strategic initiatives to protect the United States against terrorist attack across critical infrastructure sectors.

Previous to his position within the Office of Infrastructure Protection, Col Stephan served as Special Assistant to the Secretary of Homeland Security and Director of the Secretary's Operational Integration Staff. In this capacity, he was responsible for a wide range of activities that included headquarters-level planning in the areas of strategic and operational planning, core

mission integration, domestic incident management, training, and exercises. He also directed the Interagency Incident Management Group, integrating Department and interagency capabilities in response to domestic threats and incidents.

Col Stephan held a variety of key operational and command positions in the joint special operations community during a 24-year Air Force career. During Operation Desert Storm, he deployed to Saudi Arabia as a joint battlestaff planner and mission commander supporting Joint Special Operations Task Force strategic interdiction operations in Iraq. As a commander of two Air Force Special Tactics Squadrons, Col Stephan organized, trained, and equipped forces for contingency operations in Somalia, Haiti, Bosnia, Croatia, Liberia, Colombia, and Kosovo.

Col Stephan is a distinguished graduate of the United States Air Force Academy, and holds a Bachelor's Degree in Political Science. He is an Olmsted Scholar, and earned Masters' Degrees in International Relations from the University of Belgrano, Buenos Aires, Argentina, and the Johns Hopkins University.

Simon Szykman is the Director of the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD), and is responsible for the coordination of planning, budget, and assessment activities for the Federal NITRD Program, which conducts research leading to technological breakthroughs that advance the field of information technology. As NCO Director, Dr. Szykman serves as Co-Chair of the NSTC Subcommittee on NITRD, and reports directly to the White House OSTP and the NSTC.

Dr. Szykman arrived at the NCO from the United States Department of Homeland Security's Science and Technology Directorate, where he served as the Department's first Director of Cyber Security Research and Development since late 2003. Dr. Szykman joined DHS after an 18-month assignment at OSTP. In the role of senior policy analyst, he served as OSTP's liaison to the NCO and the NITRD Program.

Prior to joining OSTP, Dr. Szykman spent several years as a member of the technical staff at the National Institute of Standards and Technology.

Rod Wallace has been with Nortel for 16 years. In his current role, he leads Nortel's Global Network Security and Physical Security solutions and services business. Previously, as a Director within the Chief Technology Officer organization, he was responsible for defining and ensuring adoption of key end-to-end functional capabilities in all of the product portfolios such as: Internet Protocol version 6, network security, quality of service, and voice quality, among others.

Mr. Wallace has been a key contributor to the National Security Telecommunications Advisory Committee's Network Security Information Exchange, the Network Reliability and Interoperability Council's Cyber Security Focus Groups, the National Academy of Sciences, and many other critical infrastructure security working groups and committees.

Mr. Wallace is a board member of the Internet Security Alliance and SecureInfo Corporation.

Mike Zafirovski is President and Chief Executive Officer of Nortel, a global leader in innovative communications and services that are enabling the transformation of businesses around the world.

Since joining Nortel in November 2005, Mr. Zafirovski has drawn on his depth of global business expertise to drive sustainable business improvements that build on the company's innovative strength in new technologies that are bringing unprecedented levels of personalization, security, and mobility to communications.

Mr. Zafirovski is a 30-year business veteran with impressive global experience at two of the world's highest profile corporate innovators – General Electric (GE) and Motorola.

Prior to his current role at Nortel, he was president and chief operating officer of Motorola from July 2002 to February 2005 where he was a key player leading the company's re-emergence in innovation, market share gains, and significant profitability improvements by all six businesses. Mr. Zafirovski joined Motorola in June 2000 to lead its mobile devices business, which during his tenure returned to profitability and increased market share through the introduction of exciting new products and the Moto branding campaign.

Before his leadership positions at Motorola, Mr. Zafirovski spent 25 years at GE, including 13 years as president and chief executive officer of five businesses in the industrial, financial services, and insurance businesses. Prior to that, he held a number of increasingly senior positions in finance, auditing, marketing, and strategy/business development at various GE businesses.

Mr. Zafirovski holds a Bachelor's Degree in Mathematics from Edinboro University in Pennsylvania where he also captained the intercollegiate soccer and swimming teams. In 2002, Edinboro University awarded Mr. Zafirovski with an honorary doctorate degree. A native of Macedonia, he received the Ellis Island Medal of Honor in 2004.

Mr. Zafirovski serves on the board of directors of Boeing. An active member of civic and business communities, Mr. Zafirovski serves on several professional, educational, and non-profit business organizations, including The Canadian Council of Chief Executives, The Economic Club of Chicago, and the Macedonian Arts Council.

APPENDIX F

OFFER FOR OPEN SUBMISSION

Offer for Open Submission

A traditional call for papers was not conducted for the 2006 NSTAC RDX Workshop. Instead, participants were given the option to voluntarily submit papers related to the topic of global partnerships, preparedness, and response. Several participants have submitted papers for the exchange while others may do so in the future. Please go to http://www.ncs.gov/nstac/rd/nstac_rd_about.html for further information.

APPENDIX G

ACRONYM LIST

Acronym List

AFCEA	Armed Forces Communications Electronics
BAA	Broad Agency Announcement
BGP	Border Gateway Protocol
CBRN	Chemical, biological, radiological, and nuclear
CBRNE	Chemical, biological, radiological, and nuclear explosives
CEO	Chief Executive Officer
CIP	Critical Infrastructure Protection
CRC	Communications Research Centre
CRTI	CBRN Research and Technology Initiative
CSC	Computer Science Coporation
CSIA	Cyber Security and Information Assurance
CTO	Chief Technology Officer
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DND	Department of National Defence
DNSSEC	Domain Name Security System
DOD	Department of Defense
DRDC	Defence Research and Development Canada
EOP	Executive Office of the President
ENUM	E164 Number Mapping
EP	Electrical Power
ETSI	European Technology Standards Institute
FIPS	Federal Information Processing Standard
GE	General Electric
GETS	Government Emergency Telecommunications Service
HSARPA	Homeland Security Advanced Research Projects Agency
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronic Engineers
IES	Industry Executive Subcommittee
IESO	Independent Electricity System Operator
IIS	Information Infrastructure Security
ISAC	Information Sharing Analysis Center
IT	Information Technology
ITAA	Information and Technology Association of America
ITU	International Telecommunications Union

LOGIIC	Linking the Oil and Gas Industry to Improve Cyber Security
LMR	Land Mobile Radio
MANET	Mobile Ad Hoc Network
MITACS	Mathematics of Information Technology and Complex Systems
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
NGN	Next Generation Network
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NITRD	Network Information Technology Research and Development
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
OSTP	Office of Science and Technology Policy
PITAC	President's Information Technology Advisory Committee
PIV	Personal Identity Verification
PREDICT	Protected Repository for Defense of Infrastructure against Cyber Threats
PSTP	Public Security S&T Program
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
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
U.S.	United States
VoIP	Voice over Internet Protocol

Wi-Fi	Wireless Fidelity
WiMAX	Microwave Access
WPS	Wireless Priority Service