2004 RESEARCH AND DEVELOPMENT EXCHANGE WORKSHOP PROCEEDINGS

A YEAR LATER: RESEARCH AND DEVELOPMENT ISSUES TO ENSURE TRUSTWORTHINESS IN TELECOMMUNICATIONS AND INFORMATION SYSTEMS THAT DIRECTLY OR INDIRECTLY IMPACT NATIONAL SECURITY AND EMERGENCY PREPAREDNESS

Sponsored by the President's National Security Telecommunications Advisory Committee's Research & Development Task Force

October 28–29, 2004
Monterey, California

MEMORANDUM FOR THE INDUSTRY EXECUTIVE SUBCOMMITTEE

SUBJECT: 2004 NSTAC Research and Development Exchange Workshop Proceedings

On October 28–29, 2004, the President's National Security Telecommunications Advisory Committee (NSTAC) held its sixth Research and Development Exchange (RDX) Workshop, in Monterey, California. The purpose of the event was to:

1) Reconsider key research and development (R&D) issues related to the trustworthiness of national security and emergency preparedness (NS/EP) telecommunications and the underlying networked information systems and assess progress made in the last year;

2) Identify and frame key R&D related policy issues associated with the trustworthiness of NS/EP telecommunications and underlying information systems for future consideration and study by the President's NSTAC and research communities;

3) Provide input to the White House's Office of Science and Technology Policy (OSTP) in its preparation of the President's R&D agenda and budgetary submissions and advise the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate as it formulates research priorities and budgetary requests;

4) Discuss the roles played by industry, Government, and academia in advancing the trustworthiness issue and determine who is responsible for leading the way and implementing past and future recommendations, and which other partners are essential or desirable to effect the recommended changes; and

5) Evaluate how the R&D community can work collaboratively to effectively share information and capitalize on collective advancements as communities of interest shift.

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 several issues or concerns regarding or impacting the trustworthiness of NS/EP telecommunications and information systems, including the following: the conclusion that collaboration is essential for successful R&D initiatives; the importance of embedding ubiquitous, interoperable identity management and authentication systems into future networks; a need to examine interdependencies between critical infrastructures, especially the implications of the intersection between telecommunications and electric power; a need to influence business drivers and policy levers and provide other incentives to promote a culture of security; and a need for agreement on a common agenda to achieve progress in trustworthiness R&D.

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 Industry Executive Subcommittee and the NSTAC should continue to work with OSTP, DHS S&T, and other NSTAC stakeholders to explore key issues related to R&D of NS/EP telecommunications and information systems.

The R&D Task Force greatly appreciates the support of the OSTP, DHS S&T, and our breakout session facilitators. In particular, we thank the Associate Director of OSTP, Mr. Richard M. Russell; the DHS Under Secretary for S&T, Dr. Charles E. McQueary; the Chairman and Chief Executive Officer (CEO) of BellSouth and Chair of the NSTAC, Mr. F. Duane Ackerman; the Chairman and CEO of VeriSign and NSTAC Principal, Mr. Stratton Sclavos; and, the Vice President for Computing Sciences Research at Bell Laboratories, Lucent Technologies, Dr. Wim Sweldens for their personal engagement in the event, which greatly contributed to its success. We also thank the Naval Postgraduate School faculty members for their formidable support of the RDX Workshop. We are grateful as well to the staff that performed so well, attending to so many details. Finally, we extend many thanks to the NSTAC member companies for their resources and support.

Respectfully,

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

ACKNOWLEDGEMENTS

The President's National Security Telecommunications Advisory Committee (NSTAC) would like to thank the representatives from industry, Government, and academia who participated in the sixth Research and Development Exchange (RDX) Workshop held at the Monterey Marriott from October 28–29, 2004, in Monterey, California. NSTAC would especially like to acknowledge the important contributions of the Office of Science and Technology Policy (OSTP); the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate; the Office of the Manager, National Communications System (OMNCS); and the Naval Postgraduate School (NPS) for the planning of the 2004 RDX Workshop.

Special thanks also go to our Keynote Speakers, Mr. Richard M. Russell, Associate Director for Technology, OSTP; and Dr. Charles E. McQueary, Under Secretary for S&T, DHS; our Invited Speakers, Mr. F. Duane Ackerman, Chair of the President's NSTAC, and Chairman and Chief Executive Officer, BellSouth; Mr. Stratton Sclavos, NSTAC Principal and Chairman and Chief Executive Officer, VeriSign; and Dr. Wim Sweldens, Vice President, Computing Sciences Research, Bell Laboratories; and our panelists and breakout session facilitators from the NPS, Dr. John Arquilla, Dr. Matthew Carlyle, Dr. George Dinolt, and Dr. Cynthia Irvine. We would also like to thank our breakout session co-facilitators, Mr. David Barron, BellSouth; Mr. Frank Cantarelli, Lucent Technologies; Ms. Cristin Flynn Goodwin, BellSouth; and Mr. Michael Tiddy, Lucent Technologies.

TABLE OF CONTENTS

LIST OF APPENDICES

EXECUTIVE SUMMARY

From October 28 to October 29, 2004, the President's National Security Telecommunications Advisory Committee (NSTAC) conducted its sixth Research and Development Exchange (RDX) Workshop entitled, *A Year Later: Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness*. The purpose of the event was to stimulate an exchange of ideas among researchers and practitioners from the telecommunications industry, Government, and academia on issues regarding trustworthiness of national security and emergency preparedness (NS/EP) telecommunications systems.

Increasing reliance on the public switched network, the Internet, and computer applications to support national security, homeland security, emergency preparedness, and public safety places a premium on *trusted* systems (e.g., systems that are available, secure, reliable, and survivable even in the face of attacks, failures, or accidents). The August 14, 2003, Northeast blackout underscored the critical importance of networked information systems in supporting national crisis management and response previously demonstrated by the September 11, 2001, terrorist attacks. Ensuring that national leaders, first responders, infrastructure owners and operators, and the public receive timely, accurate, and complete information from trusted networked information systems is crucial to both national and homeland security.

To date, a majority of the research studies and activities on the trustworthiness of networked information systems have focused on vulnerabilities in cyberspace (e.g., the National Research Council's seminal report, *Trust in Cyberspace*). However, achieving and sustaining trustworthiness in those systems is jeopardized by a host of other threats (e.g., exploitation by insiders, physical destruction) that extend beyond cyberspace. As a result, the Workshop organizers chose to continue the approach developed for the 2003 RDX Workshop, reconsidering the full range of trustworthiness issues as they pertained to NS/EP telecommunications systems. Specifically, the event examined four aspects of trustworthiness:

- **Cyber Security and Software:** defending against the threat of malicious software attacks, distributed denial of service attacks, and other forms of intentional or unintentional corruption of software, such as spyware;

- **Human Factors:** ensuring that humans at all stages of the security chain, from systems designers to users, are cognizant of and able to take appropriate actions to ensure trustworthiness;

- **Integration:** managing and integrating innovative research and development (R&D) to build trusted tools and systems to support future NS/EP telecommunications infrastructures and applications; and

- **Physical Security:** protecting physical assets (e.g., facilities, equipment) from damage, destruction, and/or exploitation.

During the 2-day event, participants engaged in a facilitated dialogue including both plenary and breakout sessions. From these sessions, five issues regarding the trustworthiness of NS/EP telecommunications and information systems emerged:

- **Collaboration is essential for successful R&D initiatives.** The rapid pace of technological advancement combined with the critical importance of ensuring that NS/EP requirements are met on future networks demands increased collaboration between all stakeholders to improve the security and resiliency of telecommunications and information systems. R&D partnerships need to be created to promote cooperation and interoperation across infrastructures, sectors, and domains. 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. Economic incentives need to be created for all sectors to collaborate on R&D.

- **Ubiquitous, interoperable identity management and authentication systems must be embedded into future networks.** In the current operating environment users and the devices they employ enjoy relative anonymity on the Internet. However, to ensure improved security within a dynamic threat environment, users must be made accountable for their activities. 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 next generation network (NGN) must be conducted.

- **A need to examine interdependencies between critical infrastructures, especially the implications of the intersection between telecommunications and electric power.** New technology, business trends, regulatory decisions, and other factors all exert evolutionary pressure on the telecommunications infrastructure. As traditional circuit switched wireline telecommunications give way to Internet-based and wireless communication, reliance on power increases and the interdependence between the telecommunications and electric power infrastructures vastly expands. Additionally, the dramatic increase in communication, commerce, and interaction in today's digital society multiplies the demands placed on these super-infrastructures, which not only enable all business and economic transactions but also sustain operations across all other critical sectors. Consensus on the criticality of these functions indicates a need for increased R&D investments and the deployment of modeling, simulation, analysis, and testing capabilities to identify interdependencies and associated implications, as well as devise solutions to strengthen the foundation and alternative means for supplying reliable power sources and survivable telecommunications capabilities.

- **A need to influence business drivers and policy levers and provide other incentives to promote a culture of security.** Although the public switched telephone network (PSTN) has been subject to substantial Government regulation, economic forces have driven the development and design of the NGN. However, a posture of improved security and trustworthiness cannot be accomplished by relying solely on market forces, nor will it occur simply as a result of Government programs. Recent standards development efforts aimed at addressing security concerns do not adequately account for conflicting commercial interests. Consequently, 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.

- **Agreement on a common agenda is critical to achieve progress in trustworthiness R&D.** Historically, public research had been the primary driver for technology innovation and development in the United States. With the onset of the digital age, private deployment of resources for R&D began to equal and exceed Government investment. Recent innovations and advancements in networked information systems have brought about dynamic change, driven primarily by commercial forces. The security paradigm has not shifted to accommodate this evolving environment, thereby thwarting long-term progress. Participants, recognizing the need to carefully allocate limited resources (Government R&D funds and grants, capital investment in industry, budget cutbacks at universities), concurred that cross-sector agreement on a roadmap for future R&D expenditures, including a clear definition of roles and responsibilities, was critical.

During the plenary closing session, Dr. Charles E. McQueary, Department of Homeland Security Under Secretary for Science & Technology, challenged the four breakout session groups to prioritize their major findings and reach consensus on a single, key recommendation for immediate Government attention, R&D investment, and action.

RESEARCH AND DEVELOPMENT EXCHANGE WORKSHOP PROCEEDINGS

1.0 INTRODUCTION

The National Security Telecommunications Advisory Committee (NSTAC) is 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 October 28 to October 29, 2004, the President's NSTAC conducted its sixth Research and Development Exchange (RDX) Workshop entitled, *A Year Later: Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness*. The purpose of the event was to stimulate an exchange of ideas among researchers and practitioners from the telecommunications industry, Government, and academia on issues regarding the trustworthiness of NS/EP telecommunications systems.

1.1 Background

Increasing reliance on the public switched telephone network (PSTN), the Internet, and computer applications to support national security, homeland security, emergency preparedness, and public safety places a premium on *trusted* systems (e.g., systems that are available, secure, reliable, and survivable even in the face of attacks, failures, or accidents). The August 14, 2003, Northeast blackout underscored the critical importance of networked information systems in supporting national crisis management and response previously demonstrated by the September 11, 2001, terrorist attacks. Ensuring that national leaders, first responders, infrastructure owners and operators, and the public receive timely, accurate, and complete information from trusted networked information systems is crucial to both national and homeland security.

The National Research Council's seminal report, *Trust in Cyberspace,* defined trustworthiness as, "assurance that a system deserves to be trusted—that it will perform as expected despite environmental disruptions, human and operator error, hostile attacks, and design and implementation errors." As networks converge, trustworthiness is an increasingly important research topic in the telecommunications and computer security field. Users in industry, Government, and academia recognize the importance of having networked information systems operate and perform as expected and on a consistent basis and not be susceptible to subversion. The *Trust in Cyberspace* report also framed the challenges to developing and maintaining trustworthiness, including the correctness, security, reliability, safety, and survivability of the public switched network and the Internet; protection of the software (or "logical") elements of computer networks; and the systems, devices, and applications employed by end users.

To date, a majority of research studies and activities focused on trustworthiness have concentrated on vulnerabilities in cyberspace. However, achieving and sustaining trustworthiness in such systems is jeopardized by a host of threats (e.g., physical destruction, exploitation by insiders) that extend beyond cyberspace. As a result, the Workshop organizers chose to continue the approach developed for the 2003 RDX Workshop, reconsidering the full range of trustworthiness issues as they pertained to NS/EP telecommunications systems. Specifically, the event examined four aspects of trustworthiness:

- **Cyber Security and Software:** technologies, such as firewalls, intrusion detection systems, and virtual private networks, among others, have been researched, developed, and fielded to protect against the threat of malicious software and distributed denial of service attacks. The trustworthiness of these technologies, however, is limited by several factors, including an inability to keep pace with attack profiles, a lack of interoperability between proprietary solutions, inconsistent patch implementation, and the increasing complexity of the telecommunications network as a result of convergence activities.

- **Human Factors:** human factors pervade every aspect of trustworthiness in NS/EP telecommunications and information systems. The efficacy of any technology depends directly on the ability of humans to configure, implement, and manage it. Several factors, such as user (or human) error, the need for commercial efficiencies, effective security policies and procedures, and personnel security and background checks, influence how trust is instilled in systems.

- **Integration:** a key challenge for organizations is effectively managing and integrating systems, applications, components, and other factors in a dynamic business environment to ensure trustworthiness. The future network must efficiently manage and integrate trustworthiness despite challenges posed by the rapid pace of technological evolution; new, proprietary solutions produced by vendors and deployed by service providers; and the new applications employed by users that were never accounted for in the original design of many operating platforms.

- **Physical Security:** as the September 11, 2001, terrorist attacks clearly demonstrated, trusted systems could be compromised via damage to and/or infiltration of the physical locality in which the critical system was housed. Damage to the facility itself may be caused by a variety of environmental and human factors (e.g., hurricanes, earthquakes, cable cuts, terrorist attacks) that have the potential to destroy, disable, or corrupt trusted systems. Beyond ensuring appropriate physical protections are built into the structure and design of a facility, a second physical security concern must also be addressed—creating suitable procedures for granting trusted access. The fear exists that legitimate personnel with authorized access to critical facilities can have malicious intent for a variety of reasons.

1.2 Purpose

The purpose of the RDX Workshop was to facilitate a dialogue among industry, Government, and academia to reconsider the cyber security and software, human factors, integration, and physical security issues associated with the trustworthiness of NS/EP telecommunications and information systems that were previously discussed at the 2003 RDX Workshop. To stimulate robust discussion, facilitators and participants from the vendor, network provider, academic, and Government communities were invited to attend the 2004 Workshop to present their viewpoints.

1.3 Proceedings Organization

This Proceedings document provides an overview of the 2004 RDX Workshop. Specifically, it is divided into six sections and associated appendices:

- Section 1 presents background information on the 2004 RDX Workshop;
- Section 2 reviews the opening plenary session, the welcoming remarks from Dr. Leonard Ferrari, Associate Provost and Dean of Research, Naval Postgraduate School (NPS), the keynote addresses by Mr. Richard M. Russell, Associate Director of the White House Office of Science and Technology Policy (OSTP), and Dr. Charles E. McQueary, Under Secretary for Science and Technology (S&T), Department of Homeland Security (DHS), as well as the panel presentation from the NPS faculty members;
- Section 3 summarizes the plenary addresses from Mr. F. Duane Ackerman, Chair of the President's NSTAC and Chairman and Chief Executive Officer (CEO), BellSouth; Mr. Stratton Sclavos, Member of the President's NSTAC and Chairman and Chief Executive Officer, VeriSign; and Dr. Wim Sweldens, Vice President, Computing Sciences Research, Bell Labs, Lucent Technologies;
- Section 4 captures the observations and findings from the Workshop's breakout sessions;
- Section 5 highlights discussions from the closing plenary session;
- Section 6 presents the major findings from the 2004 RDX Workshop; and
- Appendices A – F include the Workshop agenda, speaker remarks, speaker and facilitator biographies, and other Workshop materials.

2.0 OPENING PLENARY SESSION

The opening plenary session to the 2004 RDX Workshop commenced with opening remarks from Mr. Guy Copeland, Computer Sciences Corporation and Chair of the NSTAC Research and Development Task Force (RDTF). Mr. Copeland welcomed participants to the 2004 RDX Workshop and emphasized the importance of providing practical, actionable, specific advice to Government stakeholders as they formulate their research agendas and budget submissions. He noted that the Workshop would reconsider the R&D issues associated with trustworthy NS/EP telecommunications and information systems addressed at the 2003 RDX Workshop in Atlanta, Georgia, and examine progress made, unfinished work, and new challenges identified in the past 18 months.

Mr. Copeland reviewed the agenda and format for the event and made several administrative announcements. Next, he presented a brief overview of the core missions, functions, past and current successes, and membership of the NSTAC for those unfamiliar with the organization. Mr. Copeland noted the NSTAC had conducted several RDX Workshops with representatives from industry, Government, and academia since 1991 on a variety of important R&D topics related to network security and NS/EP telecommunications. He then described the objectives for the 2004 Workshop, commenting that breakout session groups would closely examine the trustworthiness from four different perspectives: cyber security and software, human factors, integration, and physical security. Mr. Copeland concluded by reiterating the critical need for shaping actionable recommendations on emerging issues, such as the shortened response time required by the rapid and dynamic threat environment.

2.1 Welcoming Remarks—Dr. Leonard Ferrari

Mr. Copeland introduced Dr. Leonard Ferrari, Associate Provost and Dean of Research at NPS. Dr. Ferrari welcomed attendees to the Monterey Peninsula and briefly described the composition of the school, noting the substantial international student population and emphasizing the institution's shift in emphasis from traditional defense concerns to research programs related to national security.

He continued by introducing participants to several NPS initiatives related to the global war on terrorism. He described research initiatives such as the Constructive Security Approach, which has included a number of diverse programs at the Center for Information Systems Security Studies and Research (CISR) that have focused most recently on multilevel and wireless security. Dr. Ferrari also mentioned CyberCIEGE, an interactive computer game developed by CISR, which has engaged Department of Defense (DOD) and Department of Navy personnel for the purpose of providing information assurance education, training, and awareness. He also referred to the Therminator initiative, an approach to network intrusion detection that has used real traffic from operational networks to identify anomalous patterns associated with network intrusions and multipronged network probes. Among many other ongoing initiatives at NPS, Dr. Ferrari described the Maritime Domain Project, funded by Congress, that has brought together a diverse group of stakeholders including DOD, DHS, and the White House to define, design, and test maritime domain awareness and protection systems.

He closed by highlighting NPS programs in national security affairs, including the Regional Security Education Program, the Leadership Development Program, and the Information Operations Center of Excellence. In conclusion, Dr. Ferrari emphasized the importance of forming partnerships with public and private sector counterparts. Mr. Copeland thanked Dr. Ferrari for his involvement in the Workshop and noted his interest in pursuing further opportunities for formal and informal collaboration with academic institutions such as NPS in the future.

2.2 Keynote Address—Mr. Richard M. Russell

Mr. Copeland introduced Mr. Richard M. Russell, Associate Director of Technology, OSTP, and Senior Director for Technology and Telecommunications for the National Economic Council. Mr. Russell opened his remarks by thanking the President's NSTAC for the opportunity to participate in the sixth RDX Workshop, which he noted was an invaluable forum for exchanging information pertaining to telecommunications and network security R&D issues that impact the Nation's NS/EP posture. He provided a brief overview of OSTP's role in collecting information and providing recommendations to the President on technical and scientific matters. He emphasized OSTP's particular responsibility for collaborating with the National Security Council, Homeland Security Council, and Office of Management and Budget to ensure that the President receives appropriate policy advice on NS/EP telecommunications matters. Mr. Russell also remarked on OSTP Director Dr. John Marburger's role as the head of the Joint Telecommunications Resources Board, which has been responsible for bringing Federal organizations with responsibility for crisis communications together to discuss preventative actions, inform decisionmaking, and help define policy for the President.

Mr. Russell highlighted the importance of being involved in a dialogue with industry representatives and being able to exchange trusted information between the public and private sectors. He noted how a true partnership, such as that exemplified by the NSTAC and the National Communications System (NCS) National Coordinating Center for Telecommunications (NCC), was critical because although Government is responsible for providing an integrated, unified response to crises and threats, critical infrastructure owners and operators and first responders must manage the recovery, reconstitution, and mitigation efforts at the scene. Mr. Russell mentioned how since the September 11, 2001, terrorist attacks, the Administration had worked jointly with industry partners to strengthen intelligence, improve the protection of critical infrastructure and key assets, and expand support to first responders.

Mr. Russell continued by stating that recent initiatives to expand the NS/EP communications infrastructure in a converged world have included: a call by the President to make broadband technology universally accessible and affordable by 2007; a Federal Communications Commission (FCC) effort to clear out the regulatory underbrush by freeing fiber-to-the-home from legacy investments; Federal rights of way reforms; and the identification of spectrum to be auctioned for next generation wireless services to accelerate the roll out of technologies such as WiFi and e-video.

Mr. Russell explained that convergence presented new challenges and offered opportunities for economic growth. He reported that Federal R&D investments had increased 44 percent to a record $132 billion during the past 4 years. He highlighted examples of Federal programs and initiatives at many of the department and agencies that support NS/EP telecommunications, including the NCS's route diversity study, the Department of Commerce's cyber security standards development, the Department of Transportation's adaptive quarantine research project, and the Department of Energy's multi-laboratory supervisory control and data acquisition (SCADA) testbed.

Mr. Russell continued his presentation by identifying nine topic areas that OSTP believed would deserve special attention in terms of R&D investment: 1) detection and sensor technologies and related integration needs; 2) tools and techniques for the protection of assets and prevention of successful attacks; 3) entry portal security and access to assets; 4) insider threats; 5) analysis and decision support systems; 6) response, recovery, and reconstitution; 7) new and emerging threats and vulnerabilities; 8) advanced infrastructure architectures and system designs; and 9) human and social factors. He emphasized the need for technology independent solutions that could be applied in evolutionary environments and could be easily integrated into commercially available products.

During the question and answer period, Mr. Russell addressed efforts to define the term "national security emergency preparedness" and assign authority across tiers. He also noted OSTP's role in facilitating coordination among organizations to ensure interagency connectivity would be maximized. Mr. Russell concluded his remarks by highlighting several topic areas that would benefit from expedited consideration from the NSTAC, including detecting insider threats, predicting emerging threats and vulnerabilities, and improving response, recovery, and reconstitution.

2.3 Keynote Address—Dr. Charles E. McQueary

Mr. Copeland introduced Dr. Charles E. McQueary, DHS Under Secretary for S&T. Dr. McQueary opened his remarks by thanking the NSTAC for its continuing efforts toward securing the Nation's telecommunications infrastructure and noted that the NSTAC's critical thinking in identifying vulnerabilities continually impressed him. He stated that he was looking forward to the valuable output from the 2004 RDX Workshop and planned to share key lessons with his DHS colleagues. He also requested that, to make the feedback even more valuable to DHS, participants focus on developing actionable recommendations, ranking priorities, and identifying the expected results and timeline. He also recommended placing emphasis on the areas of resilience and recovery.

Dr. McQueary described the DHS mission as one designed to protect and defend the Nation against attacks that create casualties and harm the core infrastructure. He noted how DHS was protecting more than 1 billion transactions per year and must be successful each time, while a terrorist need only prevail once. To that end, Dr. McQueary stated that the Department had partnered with national labs, industry, and academia to share information and develop technologies to protect against attacks. Dr. McQueary added that although the primary focus of DHS was protection, all parties participating in homeland security must not lose sight of the need for rapid response and recovery methods.

Dr. McQueary then outlined the current organization of the Department and described the mission and leadership of each of the four directorates. He commented that S&T served a customer-supplier relationship with the other directorates, choosing tasks that were important to the other directorates, and working toward priorities that the other directorates conveyed interest in. Dr. McQueary cited the Information Analysis and Infrastructure Protection (IAIP) Directorate's National Infrastructure Protection Plan (NIPP) as an example whereby S&T provided the technologies to meet the mission of the NIPP. He mentioned that other drivers of S&T priorities included the Homeland Security Act of 2002, current threat assessments from the intelligence community, and the Homeland Security Presidential Directives (HSPD).

Dr. McQueary specifically highlighted HSPD-7 and the interagency coordination required to identify and prioritize critical infrastructures. He noted that HSPD-7 also necessitated collaboration with the private sector and information sharing regarding threats and vulnerabilities. Dr. McQueary said he believed that to be successful, Government must recognize the competitive nature of industry and employ an approach much like the Malcolm Baldridge Award, whereby industry need not share critical, proprietary details, but rather share best practices to support the infrastructure's greater good. Dr. McQueary also acknowledged the potential for successes in telecommunications and information technology information sharing methodologies to trickle down to other critical infrastructures.

Dr. McQueary then described the organization of the S&T Directorate, including the Office of Plans, Programs, and Budgets; the Office of Research and Development; the Office of Systems Engineering and Development; and the Homeland Security Advanced Research Projects Agency (HSARPA). Dr. McQueary noted that HSARPA conducted much of its work in conjunction with private industry and some with universities, taking prototypes of homeland security technologies and making them full scale. The Office of Programs, Plans, and Budget created a portfolio of efforts, some scientific such as chemical and biological, some cutting across DHS units such as emerging threats and standards, and some unit-specific such as those dedicated to cyber security and critical infrastructure protection.

Dr. McQueary transitioned his focus to highlighting several of the S&T Directorate's successful projects. He first described the critical infrastructure decision support system designed for all 14 critical infrastructures and key assets. He stated that the system mapped out types of threats and potential means of attack and was used by State and local Governments and industry and Federal decision makers to assist in planning prioritization, mitigation, and response and recovery strategies. Dr. McQueary noted a specific telecommunications industry example of potential business losses related to an attack on a critical telecommunications site whereby it would take approximately 30 days to recover and losses could approach $600 million. Dr. McQueary also noted ongoing efforts to improve cyber security, specifically highlighting joint S&T and National Science Foundation funding for a testbed to be fully operational in 2006. He stated that the testbed would be a self-contained Web site that would provide a physical network to test attack and defense methods on software.

Dr. McQueary continued his presentation by noting that under the direction of then-DHS Secretary Tom Ridge, the S&T Directorate established an Office of Interoperability and Compatibility to coordinate and enhance the emergency response capabilities of public safety officials and first responders nationwide. He explained that the purpose of the office was to set standards for wireless interoperability among the 44,000 local, tribal, and State agencies and 100 Federal agencies and public safety officials and increase compatibility in equipment and training for first responders across multiple jurisdictions. He also noted that RapidCom campaigns had been initiated in several major urban areas to boost emergency response capabilities.

Lastly, Dr. McQueary discussed current funding to fight terrorism. He noted an increase in R&D spending, including a 20 percent increase for the S&T Directorate and $13.1 billion allocated for first responder and terrorism preparedness. He said that overall, the DHS budget was up from $19.8 billion in 2001 to $40.7 billion for fiscal year 2005.

In conclusion, Dr. McQueary commented on the New York City subway system's impending 100-year anniversary. He noted that 100 years ago, pedestrian traffic was stunned to see people emerging from the underground subway system. However, he said that sight today was commonplace as subways became absorbed into our society and critical to the Nation's transportation and communication systems. He noted that—similar to anything else that would draw large crowds—subway systems were vulnerable to terrorism. Dr. McQueary further stated that the S&T Directorate had recently deployed PROTECT, a sensor system created to respond to chemical releases in subways systems in Washington, DC, and Boston. He said that the system protected 1.3 million subway riders, but had the potential to protect 8.8 million riders nationwide by halting trains, cutting off contaminated ventilation systems, evacuating riders, and providing critical information for responders.

(Note: the full text of Dr. McQueary's keynote address is attached in Appendix C)

2.4 R&D Perspectives Panel

Following Dr. McQueary's keynote address, Mr. Copeland introduced panel members from NPS. Mr. Copeland welcomed Dr. John Arquilla, Associate Professor, Defense Analysis; Dr. Matthew Carlyle, Associate Professor, Operations Research; Dr. George Dinolt, Associate Professor, Computer Science; and Dr. Cynthia Irvine, Professor, Computer Science.

Dr. Carlyle began the panel discussion with a description of the modeling and research work being done in the Operations Research department at NPS. He explained how in those programs, professors were examining critical infrastructures, with a focus on attempted attacks. He said that students had studied worst-case attacks in metropolitan areas, such as biological attacks where emergency vehicles could not reach their appropriate destinations. From that research and analysis, Dr. Carlyle shared several key insights. He noted such research had shown malicious coordinated attacks to be more damaging than natural disasters; therefore, R&D efforts should focus on using resources effectively to study possible instances of attack on critical infrastructures. In addition, Dr. Carlyle described efforts to examine redundancy in networks. He explained that system redundancy must be placed in the right location to effectively facilitate recovery efforts.

Dr. Arquilla focused his remarks on several research questions being examined at NPS. He opened by suggesting that emphasis on the trustworthiness of networks was misplaced because absolute trust was unrealizable. He referenced social networks, where nodes and members were courteous to all and confident in few. He forwarded the notion that network architecture should not be based on a presumption of trust, but built with an expectation for exploitation and deceit. Dr. Arquilla continued by expressing his belief in the need for ubiquitous, strong encryption that would improve overall security and reduce vulnerabilities. He also suggested that the R&D community examine security best practices being used in other countries. Those ideas could be used to propel R&D in the United States. Finally, Dr. Arquilla suggested examining research on weapons of mass destruction (WMD) to determine where it intersected with critical infrastructure protection. He related that observation to existing vulnerabilities in defending against physical attacks and developments in electromagnetic pulse (EMP) research.

Dr. Dinolt opened by reviewing the progress made in the R&D arena during the past year and identifying outstanding research topics that persisted. Dr. Dinolt noted that R&D constituents recognized that a security problem existed and research efforts should be focused on improvements, specifically in wireless security. In further discussion, Dr. Dinolt stated that several policy questions hindered appropriate research, including individual rights affecting identify theft, the proliferation of e-commerce vendors and merchants, and difficulties in tracking criminals appropriately. He noted that without a clear idea of the existing policies, it was difficult to determine the required mechanisms needed to defend against security violations. Dr. Dinolt also called attention to the importance of determining the appropriate security architecture for telecommunications. He noted a need for examining end-to-end encryption and the trustworthiness of several network components, including network gateways, commercial endpoints, and users. When considering identity management in the networks, Dr. Dinolt recommended that research be concentrated on binding an individual's identification to a specific institution while keeping in mind the many names people possess based on specific purposes.

Dr. Irvine concluded the panel discussion with several thoughts to incite further dialogue among participants. She noted the need to consider the trustworthiness of a shared domain for administrative and application level work. Dr. Irvine added how, in the next generation network (NGN), a logically distinct domain for administrative control could exist; however, the system must generate confidence that such a design would enable network administrators to effectively manage work. Dr. Irvine also introduced the need for understanding distributed systems and validating user actions. In her discussion, she noted that accountability should be examined by appropriately associating users with their actions. Finally, she recognized the need for secured interoperability of systems.

During the question and answer period, a participant asked about the intersection between technology and policy. Panel members replied that the tension between defending market share and protecting the Internet from fraud had added to that growing conflict. A panel member also noted the need to examine tax credits, which would enable industry to focus its resources on protecting its networks to help stop the spread of viruses and worms.

3.0 PLENARY ADDRESSES

3.1 Luncheon Address—Mr. F. Duane Ackerman

Dr. Peter Fonash, Acting Deputy Manager, NCS, again welcomed participants to the 2004 RDX Workshop and introduced Mr. F. Duane Ackerman, Chairman and Chief Executive Officer, BellSouth and Chair of the President's NSTAC. Dr. Fonash commended Mr. Ackerman for his focus on network convergence at a national level.

Mr. Ackerman opened his remarks by recognizing Mr. Russell, Dr. McQueary, and Dr. Fonash for their strong dedication to technology and support for partnerships between the research and Government communities. Mr. Ackerman underscored the need to close the gap between technology and the ability to manage the security of technology. He reiterated the strong sense of urgency from the 2003 RDX Workshop, recognized that constituents had begun to build a common agenda to meet the R&D goals defined at the Workshop, and challenged participants to move forward by extending those ideas in the breakout sessions.

Mr. Ackerman highlighted the importance of research efforts for interdependency in critical infrastructures. He referenced recent successes in the telecommunications industry during natural disasters. No central offices failed during this year's hurricanes; however, Mr. Ackerman noted that it was important to focus on the interdependence of telecommunications with other infrastructures. Mr. Ackerman also noted that increased broadband use had focused immediate importance on the interdependence between the electric power and telecommunications infrastructures. Due to the dependence of telecommunications on electric power, Mr. Ackerman noted the need for enhanced battery technology.

Shifting his focus to the NGN, Mr. Ackerman stated that it was essential for the new environment to capture the benefits of broadband use and handle forthcoming security implications. Mr. Ackerman focused on the complexity of the NGN, including its wide range of edge devices and technologies and the intricate configuration of hardware and software. As the public switched network converges with the Internet into a new environment, Mr. Ackerman noted the need to examine threats in that context, where additional endpoints would exist worldwide. He noted the importance of the role of public policy in securing investment in the new Internet, particularly the need for accelerated investment in broadband networks. Specifically, he recognized the need for additional policy focusing on technology and security.

Finally, Mr. Ackerman focused on the importance of removing barriers to establish working partnerships between industry and Government. Mr. Ackerman reflected on the idea that Government had access to the appropriate information; however, the system holding the data lacked an adequate method for processing that information. He outlined several Government working relationships that had been established, including coordination with the Alliance for Telecommunications Industry Solutions (ATIS) and the Banking Industry Technology Secretariat (BITS) to examine infrastructure interdependencies and the effective partnership of industry and Government at the NCS NCC for Telecommunications to respond to natural disasters and other catastrophes. Mr. Ackerman recognized that one positive outcome of the 2001 terrorist attacks was the subsequent unity it created within industry and the Nation. He called for participants to use that unity by acting as stewards for the infrastructures and translating research agendas into actions.

During the question and answer period, a participant inquired about how industry should balance the need to secure the NGN against the cost of doing so. He was particularly interested in how a corporation should balance national security related investments, such as redundancy, against a duty to its shareholders. Mr. Ackerman noted that without security, the Nation's economic strength was at risk. Thus, fiduciary responsibilities must be balanced against national security to ensure a healthy economic environment for corporations to thrive. The participant asked whether policy should be created to address security and to strengthen the business case. Mr. Ackerman noted that it was pragmatic for both the public and private arenas to treat security as a priority in the NGN.

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

3.2 Morning Plenary Address—Mr. Stratton Sclavos

Dr. Fonash welcomed participants back to the Workshop and thanked them for their valuable contributions to the joint dialogue. He introduced Mr. Stratton Sclavos, Chairman and Chief Executive Officer, VeriSign and NSTAC Principal. Mr. Sclavos began his presentation by talking about transformation. He noted that the United States was moving toward a digital economy and society, and that it must act to foster the next economic wave related to that profound transformation. He explained that infrastructure development had always been a driving force for U.S. society and its economy, from the construction of railroads in the 19th century to the development of electric grids, commercial aviation, and telephony networks in the 20th century, up to the surge of the Internet in the 21st century. Mr. Sclavos stated that such infrastructures had brought people, markets, information, and ideas together in ways that were previously impossible. In turn, they fundamentally had transformed commerce and communication. Mr. Sclavos highlighted the infrastructure's ability to reduce barriers of time and distance; create new ways to interact, communicate, and conduct commerce; create new services, new markets, and new relationships; and, significantly expand productivity, incomes, and standards of living.

Mr. Sclavos explained that the next great infrastructure had arrived in the form of the converged Internet and circuit switched telecommunications infrastructure. He noted that infrastructure would enable service providers, Government, enterprises, and consumers to collaborate, share, and create content, as well as communicate and conduct commerce through the use of multiple services and devices, including Web identity; e-mail; wired and wireless calls; e-commerce; extranets and intranets; and short message service (SMS).

Mr. Sclavos stated that the statistics indicated that the Internet was healthy and growing. He noted that since 2003, global Internet users had increased by 55 percent; global broadband subscribers had increased by 172 percent; U.S. e-commerce sales had increased by 58 percent; and U.S. WiFi access and client nodes had increased by 213 percent. He continued by stating that the Internet, after a period of maximum hype and then disillusionment with its potential, was now experiencing increased acceptance and serious use. He added that VeriSign had tracked a consistent rise in daily domain name server (DNS) inquiries, online merchant sales, and daily e-mail lookups during the past 3 years. He also noted how manufacturers and Government were increasingly using the Internet's capacity to deliver services and improve their efficiency.

Mr. Sclavos stated that the rise in U.S. labor productivity resulting from network convergence would dwarf any other transformation that has occurred to date as a result of an innovative infrastructure. Thus, the United States must take advantage of the global opportunities offered in the areas of communications, commerce, education, healthcare, Government, and society. Mr. Sclavos noted that the Nation must work diligently to ensure that the environment was primed to take advantage of such opportunities. In particular, he pointed to reliability, security, interoperability, regulation, and innovation as areas that must be handled correctly to create a nurturing environment.

Mr. Sclavos then discussed how great infrastructural developments transform society by enabling fundamentally new ways of communicating and conducting commerce. However, he stated that at some point in the deployment of all great infrastructures, a need for a parallel "intelligent infrastructure" would emerge. For instance, he cited how railroads needed the telegraph to reach their full potential, air travel needed air traffic control systems, utilities needed supervisory control SCADA systems, and the telephone network needed Signaling System 7 (SS7) protocol. He emphasized that basic functions of finding, connecting, securing, and transacting were fundamental to making networks truly global and interconnected.

Mr. Sclavos noted that as the Internet's influence and footprint continued to grow, so too would threats against it, such as cyber crime. In response, intelligence must be built into the network. He said that intelligent infrastructure services in the form of command, control, and coordination must be developed and offered involving robust platform sets that could provide scalability, interoperability, adaptability, reliability, and visibility, and that could be accomplished in an economically viable fashion. He explained that the complexity of intelligence must be removed from the transport layer to become invisible to the user. Accordingly, Mr. Sclavos called on stakeholders to promote innovation through the following recommendations:

- Develop and enforce policies that encourage infrastructure investment;
- Champion public/private funding and support for new technologies;
- Encourage innovation at the Internet's core;
- Promote industry-led standards and technology-independent platforms; and,
- Ensure interoperability among devices, platforms, and applications.

He also noted the importance of enabling a culture of security and trust through the following recommendations: 1) making critical infrastructure providers accountable; 2) ensuring cyber security was a must for every enterprise; 3) creating and adhering to best practices; 4) prioritizing the development of extensible authentication systems, which would have the potential to help resolve problems created by spam, phishing, viruses, and spyware; and 5) funding and promoting "Secure Internet" education at the earliest ages.

In conclusion, Mr. Sclavos noted that convergence and the next great infrastructure had arrived. He reiterated that an intelligent infrastructure would be the catalyst for future innovation and that new and real opportunities were emerging. He cautioned that stakeholders must push further ahead in regard to innovation, security, and trust techniques to help foster the next wave of technical and economic advancement.

3.3 Luncheon Address—Dr. Wim Sweldens

Dr. Fonash introduced Dr. Wim Sweldens, Vice President, Computing Sciences Research Bell Labs, Lucent Technologies, and thanked him for his commitment in support of the President's NSTAC. Dr. Sweldens opened his remarks by contrasting the critical infrastructure protection efforts in his homeland of Belgium, closely related to the size and scale of Maryland, with efforts in the United States, which have a much larger, worldwide impact. Dr. Sweldens noted that the most important trend in telecommunications is convergence of wireless and wireline and voice and data networks. He noted how, although convergence was driving efficiencies in numerous areas, there were three issues related to convergence that, if not addressed, could end up handicapping the potential of the technology: e-authentication, creating a secure and reliable backbone, and building a trusted information network.

Dr. Sweldens first noted that authentication was the most important issue in e-security today. He said that there were more than 1 billion e-mail users and currently 81 percent of all e-mail was spam. Dr. Sweldens expressed concern that as convergence became more integrated in available technologies, spam would dominate other means of communication as well. He cited examples of spam over SS7, spam over Internet telephony (SPIT), and spam over instant messaging (SPIM) as potential derivates of weak authentication technologies in the face of convergence. Dr. Sweldens said that as industry moved forward with creating the NGN, it must build in authentication technologies. He noted that the technology already existed that would prohibit Internet users from disguising their Internet protocol address. Dr. Sweldens advised industry to build authentication into the NGN rather than employ it as an afterthought. He added that every user should employ encrypted e-mail and explore single sign on technologies.

The second issue Dr. Sweldens addressed was creating a secure and reliable backbone, and he offered a three-pronged approach to this goal. The first step would include priority queuing of signaling packets that were responsible for quality of service. The second step, according to Dr. Sweldens, would be ad hoc diversity, which would not exist if access lines were carried through the same ducts. He noted that industry must conduct more fundamental mathematical work about the composition of a network and its principles. Lastly, Dr. Sweldens commented on the trustworthiness of software. He noted that functionality must be built into software to help users validate that the software was performing only the functions that it was designed to and was performing them to the highest standard.

Dr. Sweldens presented a third critical issue related to improving security in the face of convergence: building a trusted information network that allowed key people to communicate with each other and access critical information during times of crisis. As a means to reach that goal, Dr. Sweldens encouraged the use of commercially available technology, including mobile broadband communications. He noted that such a form of communication when it was applied to the upper 700 megahertz of spectrum and nationally interoperable technology would greatly increase the ability of first responders to find one another.

Concluding his remarks, Dr. Sweldens also recommended the development of doomsday scenarios where, to prevent total disaster, users would have to identify and safeguard a backup system that would allow them to access key information when all other networks failed. Dr. Sweldens noted that, in such a disaster, peer-to-peer networks and files could survive and act as a means to share critical information.

4.0 BREAKOUT SESSIONS

To facilitate discussion of trustworthiness issues, participants were asked to consider the following questions:

- What progress has been made, if any, in trustworthiness R&D since March 2003 when the last RDX Workshop was held?
- What critical challenges remain for ensuring network trustworthiness? Are those challenges the same as those raised at the last RDX Workshop? What other areas deserve consideration? Are there new challenges and issue areas not previously discussed? Are there events that have occurred since March 2003 (e.g., the Northeast blackout) that underscore additional issues to consider?
- How can the R&D community work collaboratively to effectively share information and capitalize on collective advancements that relate to trustworthiness as communities of interest shift?
- What roles should industry, Government, and academia (e.g., OSTP, DHS S&T) play in advancing the trustworthiness issue? Who should be responsible for leading the way and implementing past and future recommendations? Which other partners would be essential or desirable to effect the recommended changes? What funding would likely be necessary? From what sources?
- Based on the session discussions, what input would you provide to OSTP in its preparation of the President's research agenda and budget requests? What underlying policy issues should the President's NSTAC or other body study?
- What would be your three to four key points related to developing an agenda for action on trusted NS/EP telecommunications?

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

Breakout Session	**Facilitator**
Cyber Security and Software	Michael Tiddy, Lucent Technologies Cynthia Irvine, NPS
Human Factors	Cristin Flynn Goodwin, BellSouth John Arquilla, NPS
Integration	Frank Cantarelli, Lucent Technologies George Dinolt, NPS
Physical Security	David Barron, BellSouth Matthew Carlyle, NPS

Over the course of the 2 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. Observations and results from the breakout sessions follow.

4.1 Cyber Security and Software

Participants focused on the need for concerted R&D initiatives that would address the complex realities associated with the transition to a converged network. They indicated that it was critically important to understand interdependencies, associated threats, and correlated points of failure across critical infrastructures.

4.1.1 The Current Operating Environment

A participant noted that software was finally available in the market that would scan code and recognize vulnerabilities. The participant viewed that as a milestone, as that type of software was not viewed as commercially viable in the past. It was stated that although venture capitalists were now willing to fund such type of software development, there was still work to be done. For instance, it was noted that the software depicted only low-grade vulnerabilities, such as buffer overflows. It was suggested that additional research be conducted to further test the reliability of code scanning software.

Another participant noted that a finding had been made that A1/B1 Systems were not commercially viable. Two problems were noted involving the technology: 1) the systems were too complex and inflexible; and 2) relevant business markets, such as the defense industry, had not broadly adopted them. Participants also noted that the E17 process was inhibiting innovation and that industry should rethink the common criteria. Participants agreed that complex system and validation tools were still needed, and that additional R&D needed to be conducted in this area.

The participants then discussed coding standards and other best practices. It was noted that some companies had made progress in adopting such standards, and that they were rolling out current tools that addressed real-time interruptions. Participants added that companies had also made progress in sharing information regarding best practices because they had recognized a common interest in defending themselves against cyber-crime techniques.

In general, the group agreed that some short-term progress had been made in the area of trustworthiness R&D. Participants cited R&D advancements, including the orange book, ring architectures, common criteria, and authentication mechanisms that reported at log-on whether the device was at the right patch level. However, they concurred that long-term progress had been slow because many products were not commercially viable. Participants agreed that the complexity of today's systems with wireless technology and multiple access points had made trustworthiness an even greater challenge. It was noted that no one company could create the end secure system because, although components might be secure, a weak link could exist somewhere else along the chain. Progress was also discussed in the following areas: competitively priced trusted computer systems with enforceable encryption built into the hardware; application of stricter identifiers through code signing and Sender Policy Framework (SPF); and packet filtering.

4.1.2 Research Priorities

Participants began their discussion of critical challenges by focusing on the vulnerabilities created by home users. In particular, they discussed the risk of home users being used as bots for creating denial of service (DoS) attacks, and the gaps and vulnerabilities created by users moving from secure systems at work to nonsecure systems at home. The ease of obtaining passwords was also noted as an important problem, and it was suggested that smart cards might be a future solution.

Members also noted the potential national security implications of phishing attacks. They agreed that beyond the Global Early Warning Information System (GEWIS) and the Cyber Warning Information Network (CWIN), industry needed to receive actionable threat information. They noted that no one clearinghouse existed for disseminating information and action steps. They suggested that a research group should be recommended to Government stakeholders that would focus on gaps in cyber security and facilitate information sharing between Internet service providers (ISP), other network stakeholders, and Government agencies. It was noted by one Government participant that the DHS S&T Directorate and the OSTP were already doing work in that area.

The group discussed changes in the network control plane in a converged environment. One participant noted that the PSTN had a closely guarded control plane, which facilitated security. Others noted, however, that the changes and complexity resulting from convergence might, in the long run, provide for greater security in future networks. It was noted that research must be initiated to help determine what level of trustworthiness would be needed in the new converged environment. For instance, it was noted that A1 and B1 labeling had not proved themselves to be viable. Participants also discussed the effects the new business environment would have on trustworthiness. As the post-converged network would be based on an economic model, and not the regulated model of the past, the participants saw an important research question emerge—how trustworthiness was defined in the new business environment.

The group turned its attention to the interdependency of power and communications in the converged environment. It was noted that as providers move to cable and Voice-over Internet Protocol (VoIP), losing power would mean losing voice capabilities. The participants agreed that research should be accomplished in this area, as many had yet to grasp the seriousness and complexity of the issue.

The group also discussed a need for further research in the area of identity management, such as authentication, authorization, and priority. The group agreed that asserting identity over the network was a complex topic, and that priority in the converged environment needed to be addressed. They highlighted the differences between logical and physical access and the challenges of deploying authentication and priority on a large scale, noting that device and user identification techniques would be required for next generation networks. One participant noted that it would be useful to have the ability to dynamically raise the authority of an individual or device to access priority services during a time of crisis. With that in mind, it was questioned whether it would be enough to place priority at the edge, or whether it needed to be built into the network. Another participant noted that future priority would be offered as a contract service.

Additionally, participants discussed further research needs on the topics of encryption and filtering. In particular, encryption was discussed in the context of balancing law enforcement priorities with trustworthiness. Group members noted how filtering raised scalability and efficiency issues. They discussed how, although the network layer could perform traffic management, content management was not manageable or efficient.

A suggestion was made that a Government entity, such as the National Institute of Standards and Technology (NIST), should develop minimal audit requirements that would be tied to procurement. In such a way, the Government might be able use its buying power, as opposed to regulation, to force trustworthiness.

Participants touched on several other subjects that would require further emphasis by the R&D community, including: 1) security and reliability of the DNS; 2) Multi-Protocol Label Switching (MPLS); 3) guaranteed rates of bandwidth; 4) quality of service (QoS); 5) Secure Border Gateway Protocol (SBGP) and its ability to facilitate the "black holing" of exposed packets; 6) methods of ensuring routing registries received accurate data; 7) metadata for secure digital layer to facilitate NS/EP communications and enable multilayer information sharing, while also protecting privacy and civil liberties: and, 8) the ability of Internet Protocol version 6 (IPv6) to reduce spam.

The group also discussed several overriding issues for the R&D community, including new modeling and testing strategies for emerging technologies and the need for additional testbeds; economic impact issues; and the impact of deployment for service providers.

As a result of the discussion, participants developed a list of research priorities they believed should be further examined (see Figure 1).

Figure 1. Cyber Security and Software Research Priorities

RESEARCH AREA	RECOMMENDED TOPIC FOCUS
Convergence of Telecommunications & IP Networks Convergence of	• High assurance control plane ▪ Integrity/availability – SS7 style ▪ Logical separation for NS/EP ▪ Layer translucency for NS/EP – all responders use same devices and layer to transport data ▪ Virtual out-of-band signaling ▪ NS/EP priority access for packet networks ▪ QoS • Interoperability/security of hybrid networks ▪ Edge vs. core security (what is pushed to edge?) ▪ Route diversity ▪ Cross-band communications ▪ Mesh networking ▪ Distributed rings

RESEARCH AREA	RECOMMENDED TOPIC FOCUS
Telecommunications & IP Networks	• Critical infrastructure interdependencies and related vulnerabilities • Encryption trade-offs ▪ At the core vs. edge? ▪ As opposed to law enforcement access control? • Policy/regulatory issues ▪ Should priority be mandated? ▪ How can innovation be encouraged while ensuring service?
Identity Management: Authentication, Authorization, and Priority	• Access control • Proof of entitlement for priority • Scaling and federating key infrastructures • Authentication of people, networks, and devices • Scaling rights management • How to protect privacy, while ensuring identification, authentication, and authorization? • Nontraceability may still be required • Cloaking devices/Anonymity, i.e., identified, authenticated, but cloaked • Biometrics • Blocking and filtering bad traffic/bad users • National border control • Can we isolate the Internet to just U.S. traffic through routing and authentication? • Event notification • Trusted path/virtual private networks (VPN) • Interoperable schema for identity management
Metrics & Effectiveness Measures	• Work factor for finding bugs — what were the expenditures (in terms of time and money) to find the last number of bugs? • Enhanced metrics for secure architecture and software engineering • Situational awareness (overall health of Internet) • Need more than compliance and $ measures • Threat modeling — assessing the cost of an attack due to lack of security • Recovery • Response time for responding to bad actors • Multiple indicators • Benchmarks • Common criteria to address developmental and operational threats • Crash tests for systems • Timeliness of identifying signatures on the network
Software/Hardware Assurance	• Malware • Malicious code detection for hardware and software • Predictable composability

4.1.3 Impediments to R&D

The group agreed on key challenges and priorities for cyber security and software trustworthiness going forward. It was generally established that R&D in the area of trustworthiness and cyber security was under-funded. A recommendation was made that funding should be increased, and that efforts should be taken to ensure sufficient funds would be available in the unclassified arena. It was noted that an entire generation of research assistants had been lost due to a lack of unclassified funding.

Other key challenges and priorities included the following:

- Slow advancements in the area of cyber security and software trustworthiness because products were not commercially viable;
- Competitive constraints prohibited industry from certain collaboration;
- More collaboration and information sharing needed among stakeholders;
- Interdependencies and related vulnerabilities among critical infrastructures and communications providers must be explored further and understood;
- Parameters for trustworthiness in the changed business environment must be developed; and,
- Encryption and law enforcement equities must be studied and weighed.

4.1.4 The Path Forward

Participants identified three areas of future research necessary to improve cyber security and software:

- **Articulate, fund, and promote R&D initiatives that consider shifting and emerging NS/EP capabilities and requirements in a converged environment.** Participants noted how several different requirements merited additional attention from the R&D community, including cross-band communications and priority on packet switched networks. Group members suggested that research on authentication, authorization, and prioritization in a converged environment was critical to securing application and transport availability end-to-end. Additionally, members mentioned how metrics for assessing performance, security, and reach of converged networks should be developed to ensure NS/EP requirements would be met. They added it was also important to extend the utilization of cyber and physical sensors and early warning systems to maintain NS/EP requirements in the NGN environment.
- **Research critical interdependencies and vulnerabilities that can affect NS/EP objectives.** Participants noted that exploring the impact of interdependencies between critical infrastructures, especially the reliance of communications on power and pipelines in NS/EP situations, was crucial to improve the security and trustworthiness of networked information systems. Group members emphasized that technologies must be developed to guarantee service availability. They suggested that threat modeling and model validation techniques should also be employed.
- **Explore the creation of baseline audit and forensic standards and analysis and study the ability of incentives to increase use.** Participants suggested that Government, through a group such as the NIST, should develop minimal audit requirements that would be tied to procurement and thereby enable Government to use its buying power, as

opposed to regulation, to force trustworthiness. Group members noted that the Government, by creating economic incentives for increased control and protection, could encourage the development and deployment of stronger audit and forensic technologies and thus strengthen the market for security.

4.2 Human Factors

Participants emphasized the fact that human factors pervaded all aspects of trustworthiness in NS/EP telecommunications and information systems. In particular, participants noted that the human element was a vital component when considering efforts to develop, maintain, and sustain trustworthiness in NS/EP telecommunications and information systems. Group members noted that the efficacy of any technology directly depended on the ability of humans to design, develop, configure, implement, and manage it. They stated how even the best technical solution could prove vulnerable to intentional (e.g., external attack, insider threat) or unintentional acts (e.g., defective software, inadequate system configuration, noncompliance with security policies). Participants concluded that absolute trustworthiness could not be guaranteed, and systems could never be fully protected; therefore, clear metrics and standard criteria must be developed to measure the value of trust against other NS/EP requirements in the new security paradigm.

4.2.1 The Current Operating Environment

A major theme in the Human Factors session was a strong sense of urgency and call to action. Participants underscored the need for engendering collective action and advancing a culture of security. They noted that little progress had been made in trustworthiness R&D that focused on human factors during the past year. Participants identified five broad areas shaping the current operating environment that affected efforts to minimize the risk of inadvertent failures and malicious acts:

- **Education, Training, and Awareness:** participants indicated that ensuring system users, senior managers, and system administrators were sufficiently prepared for incidents, understood the potential implications of attacks, and were familiar with relevant security policies, processes, and procedures were key factors in building trustworthiness. Specifically, participants observed that individuals tended to devalue self-reliance and deflect responsibility for personal security to external agents rather than taking precautions to protect themselves.

- **Policy Development, Dissemination, and Enforcement:** participants cited the lack of widely promulgated best practices for developing comprehensive security policies and uneven compliance and enforcement programs across enterprises as factors that could result in significant vulnerabilities. Participants agreed that ensuring security policies were developed and transmitted to all staff, and that their implementation was enforced, remained important aspects of maintaining trustworthiness. Participants also recognized the importance of creating incentives for exchanging institutional knowledge to counter the legal and cultural barriers to information sharing.

- **Authentication and Identity Management:** participants underscored the critical importance of developing and building interoperable, ubiquitous authentication into the NGN. They recognized that operational users and the devices that they employ undervalued the importance of controlling and managing their online identities. Participants noted that users usually enjoyed relative anonymity on the Internet, but they agreed that that privilege would be eradicated by security requirements that necessitated accountability and verification. Participants recognized the need for additional research focused on usable, multilayered identity management and credentialing technologies and methodologies that provided enhanced end-to-end authentication of users and devices in the NGN.

- **Cultural Shifts:** participants identified the basic requirement for influencing a cultural shift that would encourage users and managers alike to embrace security and reverse trends that celebrated malevolent activity or promoted reactive measures. Specifically, participants emphasized the importance of establishing a public education campaign coupled with training and awareness programs that would identify and convey the requirements for, and responsibilities of, an *ideal* user, heighten the sensitivity of employees to security concerns, and raise the perceived value of acting in favor of the common good.

- **Source of Supply:** participants noted the importance of being able to determine whether a software application or element of the architecture was designed and produced by a trusted source. Participants stated their concern was that a "bad actor" could introduce one or more vulnerabilities into software code or a piece of the larger architecture that could be exploited at a later date. Participants also discussed the need to develop a process to enforce strict code attribution and integrity controls.

4.2.2 Research Priorities

As a result of the discussion, participants developed a list of research priorities they believed should be further examined (see Figure 2).

Figure 2. Human Factors Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Optimal Hybridization of Decision Systems	• Reduce impact of human factors (e.g., number of humans interfacing with key systems) by making security transparent and leveraging mechanized response tools where appropriate • Enhance tools and technologies to improve human decisionmaking under conditions of ambiguity or uncertainty • Employ modeling techniques to understand the correct balance of manual and automated interactions
Authentication and Identity Management	• Research usable, multilayered identity management and credentialing technologies and methodologies that provide enhanced end-to-end authentication of users and devices in the NGN • Research tools to better interpret, authorize, and identify multifaceted users and devices with various identities/profiles • Explore legal implications (e.g., privacy) that inhibit full accountability

RESEARCH AREA	RECOMMENDED FOCUS
Education, Training, and Awareness	• Educate, train, and increase awareness of security issues (e.g., articulate and disseminate the *ideal* user profile – responsibilities, roles, and requirements) • Investigate incentives and impediments that affect a user's willingness to delegate responsibility rather than preserve self-reliance • Research the barriers that prevent wider promulgation and enforcement of best practices
Risk Management Approach to Improved Security	• Acknowledge that absolute trustworthiness is an unrealizable goal • Research and establish a risk management framework that assesses consequences and measures security using standardized criteria • Research cultural, psychological, technical, and organizational factors that build confidence in the integrity and reliability of data and systems

4.2.3 Impediments to R&D

The Human Factors session identified three overarching impediments to building trusted NS/EP telecommunications and information systems. First and foremost, they agreed that trust in the fullest sense was an unrealizable goal, and thus its importance was overstated. Participants discussed the need to find alternative methods to ensure security and build confidence in the integrity of telecommunications and information systems without achieving absolute trust. They recognized the need to use a risk management framework that would employ standard criteria to assess the severity of consequences. Participants recognized that certain NS/EP situations would require trading a reasonable amount of security for availability and agreed that it would be useful to have a methodology to measure assumed risks.

Second, participants described the need to quantify the value of security and articulate the profile of an ideal user. They agreed that wide public recognition of the importance of comprehensive security practices and personal responsibility for protection was often lacking. Participants recognized that high-end technical solutions often offered better "fixes" to security vulnerabilities, but might be costly, difficult to use, and too technically complex for the average system user. A common problem cited during the session was that the average user did not have adequate knowledge of information security and appropriate computing behavior, due in part to current tendencies to react to threats rather than take proactive measures to reduce vulnerabilities and make systems more resilient.

Third, a host of legal, jurisdictional, organizational, and cultural issues emerged as significant impediments. Specifically, discussions focused on the need to: 1) create incentives for information sharing among industry, Government, and academia to stimulate the promulgation of best (and notification of worst) practices; 2) carefully consider legal issues (e.g., reasonable expectations for privacy, concerns about liability) as they related to authentication and identity management policies; and 3) study the psychological and sociological motivations that drove people to subvert and exploit technology as opposed to those that promoted positive behavior that enhanced the collective good.

4.2.4 The Path Forward

Participants identified five areas of future research necessary to improve human factors:

- **Research usable, cost effective, and interoperable multilayer technologies for authentication and authorization.** Participants emphasized the importance of creating a single, accepted standard for authentication. They noted how highly reliable, fully trustworthy systems would be difficult, if not impossible, to achieve. Therefore, they stated that a universally accepted methodology for ubiquitous, embedded identity management and authorization of users and devices would be critical to the security of the NGN. Participants acknowledged the need to consider expectations for privacy when implementing new technologies.

- **Study methods for creating a culture of security.** Participants determined that the public was generally disinterested with its safety and security on the Internet. They discussed how users were all too willing to delegate responsibility for enhanced protection against security threats to vendors, service providers, and Government. Thus, they noted it was critically important to elevate the value of security in general and educate common users about their personal responsibility to control and manage their identity, actively defend their systems, and contribute to the common good. Participants suggested inserting information security education into the public school curriculum and mounting a public awareness campaign that would characterize and convey the profile of an *ideal* user.

- **Examine the optimum hybridization of decision systems.** Participants highlighted the need for a carefully balanced division of labor between humans and machines in reacting and responding to crises. They noted the capacity to process information about, and make decisions on, security matters was a crucial element in ensuring trustworthiness. Participants stated that human intervention was critical to some recovery and reconstitution processes; however, judgment was often compromised under conditions of uncertainty. In other circumstances, however, automated mechanisms could replace human processing and produce effective and efficient decisions in a more affordable, simplified manner that would eliminate the possibility for human error.

- **Explore methods for creating a market for security.** Participants commented that the current economic environment limited the amount of investment available to address security R&D concerns. Research into incentives (e.g., tax credits) and/or other stimulus (certification of companies) might help generate a more robust market for security. Additionally, agreement on standard metrics and criteria would allow for performance measurements across networks, systems, and sectors, stimulating industry-wide assessments and creating commercial competition for implementing strong security practices.

- **Research preemptive tactics and strategies for information security.** Participants discussed the need to examine how employing preemptive tactics and strategies, such as strict code attribution and innovative integrity controls, might deter both insider threats and external attacks. They also recognized the need to understand how technologies such as Internet relay chat (IRC) were subverted and to investigate the implications of their elimination.

4.3 Integration

Participants emphasized the importance of leveraging existing technologies and considering their utility in the transitional phase, while understanding that the NGN environment is a rapidly evolving technological frontier. In particular, participants noted an overall concern for ensuring the trustworthiness of the network, including trust between critical infrastructures, among industry and Government, and within the physical and cyber infrastructures.

4.3.1 The Current Operating Environment

The Integration session participants expressed satisfaction with progress made in the past year to advance and ensure the trustworthiness and interoperability of the network; however, participants also agreed that new research should examine trustworthiness in the changing technological environment. They identified three specific instances of progress made toward characterizing the current environment and achieving secure, interoperable systems.

- **Testbeds:** participants agreed that several testbed initiatives had been implemented successfully during the past year. They discussed the development and successes of several testbeds jointly funded by the National Science Foundation (NSF) and DHS, including the Cyber Defense Technology Experimental Research (DETER) testbed and the Evaluation Methods for Internet Security Technology (EMIST) testbed. Participants also noted the need to expand those testbeds or develop additional ones where companies could come together to conduct research while protecting their individual intellectual capital.

- **Priority Service:** participants noted that priority services were good examples of situations where industry and Government successfully worked together to achieve a common goal. They cited several examples, including the Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Special Routing Access Service (SRAS), to showcase successes and define the need to continue such services into the NGN.

- **NGN:** participants agreed that the NS/EP community's focus had transitioned from securing the traditional voice telecommunications network into securing the converging NGN. They expressed concerns over the inadequate attention given to the importance of signaling and authenticating infrastructures in the telecommunications environment over the years. They noted how a challenge existed to examine such concerns within the changing interoperability of the NGN environment.

4.3.2 Research Priorities

As a result of the discussion, participants developed a list of research priorities they believed should be further examined (see Figure 3).

Figure 3. Integration Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Network Survivability	• Conduct modeling and simulation of an integrated, survivable network in a testbed. Modeling and simulation should include, but is not limited to, recovery, reconstitution, and prioritization of access and traffic
Authentication	• Define authentication techniques in the NGN
Network Security	• Examine interoperable authentication of parties and devices • Enhance tools and techniques to achieve the necessary identity and scalable key management
Infrastructure Interdependency	• Conduct a joint cross-sector exercise with public and private industries, where physical and cyber dependencies would be examined simultaneously
Policy Development	• Improve policy framework to guide evolution of telecommunications infrastructure, including NS/EP • Examine options for how the Government could provide incentives to industry to ensure new systems and technologies could integrate with one another • Identify approaches to prepare to deal with 'high impact – low probability' events
Economic Incentives	• Investigate investment incentives to support excess capacity in the network to ensure sufficient bandwidth when needed
Priority Routing	• Develop standards to integrate token-based authentication to enable appropriate priority-based bandwidth and resource utilization

4.3.3 Impediments to R&D

Although participants agreed that progress had been made to increase the trustworthiness and interoperability of systems, they also noted several impediments to success. The group noted that a capability did not exist to illuminate interdependencies through a description of the critical infrastructures, including assets locations and information regarding collocations. Without a defined description of interdependencies, participants noted the increasing difficulty in engaging research around those interdependencies, including identifying parties to be responsible for examining interdependency concerns. Moreover, one participant pointed out the lack of an interdependency direction made it difficult to make recommendations at the Presidential level.

Participants also noted a concern over the lack of a research plan to test the fallibility of the existing Internet because of a prevailing belief that portions of the network could be disrupted, but the network as a whole could not be destroyed. Given the complexity of the Internet, participants noted a need to define which critical areas would be most vulnerable and require prompt examination. Participants were concerned that the benefits for rapid prototyping and testbeds discussed during the 2003 RDX Workshop had not yet been fully realized. They expressed that a need existed to integrate research from diverse industries, academia, and the Government to define the plan.

Participants observed that there was a lack of qualified and educated people to reconcile networks under attack. They noted that a research agenda needed to be defined to develop a range of human capital so those networks could be managed appropriately. However, the group did note that the private sector and some universities were aware of this challenge; therefore, they had developed several academic programs to achieve such knowledge.

4.3.4 The Path Forward

Moving forward, participants in the Integration session made several suggestions to advance trustworthiness in research efforts. They concentrated on the need for more productive and more focused information sharing and analysis.

Through the discussion, participants outlined several roles and responsibilities for each sector to contribute to that would enhance collaboration among key stakeholders (see Table 1).

Table 1. Research Contributions by Sector

SECTOR	ROLES AND RESPONSIBILITIES
Academia	• Educate the next generation of human capital to manage integrated systems while under suspected attack • Develop basic and generic applied research methods and ideas • Test methodologies to attack and defend very large networks
Industry	• Share research priorities with academia and the Government • Provide asset data, threat data, and scenarios for collaborated exercises
Government	• Provide asset data, threat data, and scenarios for collaborated exercises • Provide predictable funding profiles for long-term research and development priorities

Participants identified three areas of future research necessary to improve integration:

- **Conduct joint exercises to examine interdependencies.** To enhance collaboration among the sectors and critical infrastructures, participants discussed the importance of conducting joint exercises to examine interdependencies between systems. Participants emphasized the importance of examining the impacts of both physical and cyber infrastructure simultaneously during the exercise. Goals of the exercise should focus on understanding interdependencies of the integrated network, including architectural, sector, and user environments.

- **Increase research on system interoperability.** Participants also noted the need for increased research on system interoperability. Some participants suggested that Government regulation force interoperability; however, other participants argued that service providers had the choice to deploy different types of equipment based on their own needs. Participants mentioned the SS7 network and protocol as an example of an infrastructure based on interoperability. They noted how the SS7 architecture had been successful: although no requirements or mandates for interoperability had been forced onto service providers, informal industry coordination did occur.

- **Ensure service priority availability in an integrated network.** Participants determined an investment plan should be developed to ensure that the secure network architecture required for NS/EP services and the continuity of Government was achieved. Discussion focused on the most critical point in the integrated network—the signaling and backbone components. Participants commented that future research surrounding service priority availability should be based on the current assumed threat environment.

4.4 Physical Security

The Physical Security session began its discussion by acknowledging that physical threats remained a top concern for protecting the Nation from terrorist threats. However, participants also acknowledged that physical and cyber security issues were, in many ways, growing to become a singular problem. Participants discussed specific mechanisms, tools, and strategies to promote physical security. They also conducted a broad discussion of criticality and the difficulties in protecting critical infrastructures based on a changing and varied definition of the term.

4.4.1 The Current Operating Environment

Participants noted that progress had been made in trustworthiness R&D since the March 2003 RDX Workshop. In particular, the group discussed the work of the Trusted Access Task Force (TATF) of the NSTAC. They stated that the TATF had drafted recommendations to the President regarding background screening and credentialing standards for those requiring access to critical telecommunications facilities. In addition, they noted how the NSTAC's Legislative and Regulatory Task Force (LRTF) and the Network Security Information Exchange were examining the availability of critical information on physical security in the public domain. Group members also noted that various national labs (such as Los Alamos and Sandia) were undertaking modeling and simulation activities toward defense of networks and critical infrastructure and much of that work had NS/EP implications. Participants discussed how—due to the overwhelming drive to identify affordable and effective uses of biometrics technologies—groups across industry, academia, and Government, including DHS and DOD, were conducting R&D activities in the biometrics field. Lastly, while the group was unable to identify specific examples, the participants noted that there was likely progress in the anomaly detection field.
Breakout session participants identified several overarching themes affecting the physical security arena:

- **Defining "Criticality":** the group stated there was a lack of clarity and agreement on the subject of criticality. Specifically, participants discussed the need to define the term "critical," taking into account the different missions (homeland defense, NS/EP, national economy, and customer service) that an infrastructure would serve. The group recognized that the definition would drive investment, risk assessments, and response and recovery efforts, as well as aid in determining what information would be acceptable for the private sector to share via the public domain.

- **Electric Power and Telecommunications Infrastructures Interdependency:** participants discussed recent events such as the Florida hurricanes and the Northeast blackout as examples of incidents where interdependence had created vulnerabilities. The group also noted that electric power had grown as dependent on the physical backbone of the telecommunications infrastructure as telecommunications had on electric power. In particular, participants cited the reliance of telecommunications facilities on diesel fuel in the event of a power outage and the need to identify other sources of sustainable power for telecommunications facilities, as diesel fuel would only support the facilities for a limited amount of time. Participants also cited the example of cellular phones in a power outage where towers had backup power, but phones had no alternative means for recharging and therefore provide only limited service time.

- **Impact of Nontraditional Communications Technologies:** the group also discussed the proliferation of nontraditional communications technologies (wireless, cable, etc.) and the lack of standards relating to redundancy and service levels. The group examined, in the case where telecommunications was provided by nontraditional technology, the need for policy around minimum service level agreements for network redundancy and reconstitution in the case of an outage.

- **Threat-Specific Information Sharing:** participants emphasized the need for Government to share specific threat and vulnerability information with industry. The group acknowledged, however, that industry had not yet defined what type of specific threat and vulnerability information it needed from the Government.

4.4.2 Research Priorities

As a result of the discussion, participants developed a list of research priorities they believed should be further examined (see Figure 4).

Figure 4. Physical Security Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Vulnerability Analysis	• Define “criticality” and identify which assets are critical based on the defined primary mission of the infrastructure • Determine the “shelf life” of vulnerability assessments and define the parameters to identify an outdated assessment • Understand how much physical diversity and redundancy already exists and how much is necessary for critical processes and dependencies (financial services, 911 services, etc.); use this information to work toward the balance between redundancy and hardening investments
Critical Infrastructure Interdependencies	• Model physical interdependencies within the infrastructure and with other infrastructures, specifically electric power— ▪ Identify alternative means to supply power to critical telecommunications facilities and specific telecommunications components ▪ Examine electric power infrastructure dependence on telecommunications. Do they currently have and do they need to maintain some level autonomy?
Response and Recovery	• Develop response and recovery processes for physical facilities based on the definition of criticality and known interdependencies (processes, training, and technologies)
Modeling and Simulation	• Use simulated exercises, complex models, and testbeds to understand the effects of catastrophic events and test responses (gauge their speed and effectiveness)

Information Sharing	• Define industry's essential elements of information for law enforcement and intelligence to provide back to industry • Establish public/private partnerships to specifically support R&D and identify means for industry to be more involved in this work and for the Government to provide feedback to industry on progress • Define Web site publishing guidelines to minimize sharing critical information on the public network
Anomaly Detection	• Develop industry-wide guidelines on the integration of physical early warning information. Specifically, identify ways for the telecommunications industry to utilize early warning, anomaly detection, and sensor technologies from chemical, biological, and nuclear weapons research
Biometrics	• Continue biometrics R&D toward ease of use and cost reduction for the telecommunications industry

4.4.3 The Path Forward

Participants identified four areas of future research necessary to improve physical security:

- **Provide clarity on the subject of criticality.** Participants noted that various organizations had begun the process of identifying critical assets, however, as discussion progressed, the group acknowledged that the definition of critical could vary based on the function the asset served. The group noted that additional work in that area was needed, and academia, industry, and Government each had a role to play in the effort by providing a medium for dialogue and agreement, developing standards for criticality, and creating models to challenge the definition of critical assets. Participants mentioned how the agreed upon definition of critical could be used as the basis for developing risk assessments and challenging response and recovery plans.

- **Examine mutual dependency between the electric power and telecommunications infrastructure.** Participants noted that, moving forward, the growing interdependence between the electric power and telecommunications infrastructures could potentially become the greatest source of vulnerability for both infrastructures, including those that depended on them. Members suggested that further evaluation of the points of interdependence between the two critical infrastructures was needed. They offered that Government should facilitate cross-sector collaboration and exercises, academia should model the infrastructures, and telecommunication industry groups should work with electric power industry groups to share interdependency and vulnerability information.

- **Respond to the proliferation of nontraditional communications technologies and the lack of standards relating to redundancy and service levels.** Group members noted how, in recent years, communications technologies had broadened to include nontraditional technologies, such as wireless and cable equipment, potentially implemented without service level agreements to address physical security concerns. To address that issue, the group recommended that industry and Government further explore the current state of service level agreements and examine the need for new policies that would ensure minimum service level agreements accounted for network reconstitution by service providers.

- **Create guidelines for effective information sharing, specifically between industry and Government regarding threats and vulnerabilities.** Group members emphasized that continued information sharing between industry and Government was critically important. To further protect the telecommunications infrastructure, members suggested it was advisable to continue on the path of information sharing by endorsing efforts on the part of industry, Government, and academia to identify what types of threat and vulnerability information was useful to industry. Government should identify means to share specific, timely, and actionable threat information, including general threat environment information, with those industry and academic organizations conducting modeling and testbeds.

5.0 CLOSING PLENARY SESSION

The closing plenary of the RDX Workshop began with presentations from the facilitators from each breakout session. Following those briefings, Mr. David Barron, Chair of the NSTAC Industry Executive Subcommittee, thanked participants for their contributions. He commended all attendees for the progress made and the success achieved by delivering focused, specific recommendations to key stakeholders. He reiterated three themes that pervaded the Workshop —urgency, partnership, and trust—and then invited Dr. McQueary to offer his closing remarks.

Dr. McQueary again thanked Workshop participants for their dedication of resources and outlay of effort. He closed by identifying four overarching observations that were reiterated during the course of the 2-day event:

- Engaging a large and diverse number of partners is critical to the development of innovative, holistic solutions. The telecommunications industry must engage new and multiple networks of users, vendors, researchers, technologists, and critical infrastructure owners and operators to improve awareness of cross-sector vulnerabilities and interdependencies and to initiate inventive, original approaches and solutions that capitalize on answers found in other disciplines (e.g., chemistry, biology);

- Developing improved technologies, tools, and techniques to authenticate identities on the network is a commonly articulated requirement that translates to various realms, including border inspections and container security. Network architects and software designers must broaden their perspective and use lessons from the physical world to develop crosscutting methodologies and solutions;

- Considering the new vulnerabilities, accelerated threats, and shortened response time engendered by the rapid inception of the NGN, the Nation must employ caution in engineering a gradual transition that allows for consideration of NS/EP concerns such as reliability, integrity, survivability, and assurance; and

- Creating a strong business model to ensure progress, rather than relying on technologists as the driving force, is crucial for the economic health of the Nation.

Dr. McQueary followed up the four observations by challenging the breakout session groups to consider prioritizing their major findings and to reach consensus on a single, key recommendation for immediate attention, R&D investment, and action. Dr. McQueary closed the 2004 RDX Workshop by reading from OSTP Director Dr. Marburger's concluding remarks from the 2003 RDX Workshop. He congratulated participants for meeting the challenge of bringing new ideas and innovative approaches to the table for discussion. He expressed his appreciation for Dr. Marburger's wisdom, illustrated by the closing statement he delivered at the end of the previous Workshop that forecasted a clear focus and line of responsibility for security R&D issues within the Government thanks to the creation of DHS. Dr. McQueary closed by agreeing to provide feedback on the consequences of the recommendations forwarded to DHS as a result of the Workshop.

6.0 EXCHANGE FINDINGS

The R&D Exchange Workshop offered a forum for representatives from industry, Government, and academia to share their insights and perspectives on issues of security and trustworthiness. From the plenary and breakout discussions, five issues regarding the trustworthiness of NS/EP telecommunications and information systems emerged:

- **Collaboration is essential for successful R&D initiatives.** The rapid pace of technological advancement combined with the critical importance of ensuring that NS/EP requirements are met on future networks demands increased collaboration between all stakeholders to improve the security and resiliency of telecommunications and information systems. R&D partnerships need to be created to promote cooperation and interoperation across infrastructures, sectors, and domains. 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. Economic incentives need to be created for all sectors to collaborate on R&D.

- **Ubiquitous, interoperable identity management and authentication systems must be embedded into future networks.** In the current operating environment users and the devices they employ enjoy relative anonymity on the Internet. However, to ensure improved security within a dynamic threat environment, users must be made accountable for their activities. 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 must be conducted.

- **A need to examine interdependencies between critical infrastructures, especially the implications of the intersection between telecommunications and electric power.** New technology, business trends, regulatory decisions, and other factors all exert evolutionary pressure on the telecommunications infrastructure. As traditional circuit switched wireline telecommunications give way to Internet-based and wireless communication, reliance on power increases and the interdependence between the telecommunications and electric power infrastructures vastly expands. Additionally, the dramatic increase in communication, commerce, and interaction in today's digital society multiplies the demands placed on these super-infrastructures, which not only enable all business and economic transactions but also sustain operations across all other critical sectors. Consensus on the criticality of these functions indicates a need for increased R&D investments and the deployment of modeling, simulation, analysis, and testing capabilities to identify interdependencies and associated implications, as well as devise solutions to strengthen the foundation and alternative means for supplying reliable power sources and survivable telecommunications capabilities.

- **A need to influence business drivers and policy levers and provide other incentives to promote a culture of security.** Although the PSTN has been subject to substantial Government regulation, economic forces have driven the development and design of the

NGN. However, a posture of improved security and trustworthiness cannot be accomplished by relying solely on market forces, nor will it occur simply as a result of Government programs. Recent standards development efforts aimed at addressing security concerns do not adequately account for conflicting commercial interests. Consequently, 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.

- **Agreement on a common agenda is critical to achieve progress in trustworthiness R&D.** Historically, public research had been the primary driver for technology innovation and development in the United States. With the onset of the digital age, private deployment of resources for R&D began to equal and exceed Government investment. Recent innovations and advancements in networked information systems have brought about dynamic change, driven primarily by commercial forces. The security paradigm has not shifted to accommodate this evolving environment, thereby thwarting long-term progress. Participants, recognizing the need to carefully allocate limited resources (Government R&D funds and grants, capital investment in industry, budget cutbacks at universities), concurred that cross-sector agreement on a roadmap for future R&D expenditures, including a clear definition of roles and responsibilities, was critical.

APPENDIX A: AGENDA

RDX Workshop Agenda

Thursday, October 28, 2004

7:00 – 8:00	a.m.	Registration/Continental Breakfast
8:00 – 10:00	*a.m.*	*Opening Plenary Session*
8:00 – 8:20	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 (R&D) Task Force
8:20 – 8:30	a.m.	Remarks from the Naval Postgraduate School (NPS) — Dr. Leonard Ferrari, Associate Provost and Dean of Research, NPS
8:30 – 8:35	a.m.	Introduction of Keynote Speaker — Mr. Copeland
8:35 – 9:15	a.m.	Keynote Address — Mr. Richard M. Russell, Associate Director for Technology, Office of Science and Technology Policy
9:15 – 9:20	a.m.	Introduction of Keynote Speaker — Mr. Copeland
9:20 – 10:00	a.m.	Keynote Address — Dr. Charles E. McQueary, Under Secretary, Science and Technology Directorate, Department of Homeland Security (DHS)
10:00 – 10:30	a.m.	Coffee Break
10:30 – 11:45	*a.m.*	*R&D Perspectives Panel*
10:30 – 10:35	a.m.	Introduction of Panelists — Mr. Copeland
10:35 – 11:35	a.m.	R&D Perspectives Panel — Dr. John Arquilla, Associate Professor, Defense Analysis, NPS; Dr. Matthew Carlyle, Associate Professor, Operations Research, NPS; Dr. George Dinolt, Associate Professor, Computer Science, NPS; Dr. Cynthia E. Irvine, Professor, Computer Science, NPS
11:35 – 11:45	a.m.	Concluding Remarks & Introduction of Breakout Sessions — Mr. Copeland
12:00 – 1:00	*p.m.*	*Lunch*
12:15 – 12:20	p.m.	Introduction of Luncheon Speaker — Dr. Peter Fonash, Acting Deputy Manager, National Communications System, DHS

12:20 – 12:45	p.m.	Luncheon Address — Mr. F. Duane Ackerman, Chairman and CEO, BellSouth and Chair of the NSTAC
1:00 – 5:00	*p.m.*	*Breakout Sessions on Cyber/Software, Human Factors, Integration Issues, and Physical Security*
2:30 – 3:30	p.m.	Refreshments

Friday, October 29, 2004

7:30 – 8:30	a.m.	Registration/Continental Breakfast
8:30 – 9:05	*a.m.*	*Morning Plenary Address*
8:30 – 8:35	a.m.	Introduction of Plenary Speaker, Dr. Fonash
8:35 – 9:05	a.m.	Plenary Address – Mr. Stratton Sclavos, Chairman and CEO, VeriSign and NSTAC Principal
9:15 – 11:40	*a.m.*	*Breakout Sessions (continued)*
10:00 – 10:30	a.m.	Coffee Break
11:45 – 12:45	*p.m.*	*Lunch*
12:00 – 12:05	p.m.	Introduction of Luncheon Speaker, Dr. Fonash
12:05 – 12:30	p.m.	Luncheon Address — Dr. Wim Sweldens, Vice President, Computing Sciences Research, Bell Labs, Lucent Technologies
1:00 – 3:20	*p.m.*	*Closing Plenary Session Moderated by Dr. McQueary*
1:00 – 2:00	p.m.	Facilitator Reports on Breakout Sessions
2:00 – 2:50	p.m.	Question and Answer Period
2:50 – 3:20	p.m.	Plenary Closing Remarks — Dr. McQueary
3:20 – 3:30	p.m.	Workshop Closing Remarks — Mr. Copeland

APPENDIX B: ATTENDEES

Attendees

F. Duane Ackerman	BellSouth
Francis Afinidad	Naval Postgraduate School
Michael Aisenberg	VeriSign Inc.
Bora Akyol	Cisco Systems
Peter Allor	Internet Security Systems, Inc.
Jenine Alston	Booz Allen Hamilton
John Arquilla	Naval Postgraduate School (Facilitator)
David Barron	BellSouth (Facilitator)
James Bean	Verizon
Tim Bowe	Sprint
Michael Boyden	Science Applications International Corporation
Susan Brenner	University of Dayton
Shelly Brown	Booz Allen Hamilton
Charles Brownstein	Computer Science and Telecommunications Board
Bill Brykczynski	Science and Technology Policy Institute
Jonathan Burke	Georgia Tech
Karen Burke	Naval Postgraduate School
Frank Cantarelli	Lucent Technologies (Facilitator)
Matthew Carlyle	Naval Postgraduate School (Facilitator)
Christine Cermak	Naval Postgraduate School
Anne Clunan	Naval Postgraduate School
Erin Comer	Booz Allen Hamilton
Robert Connors	Raytheon
Guy Copeland	Computer Sciences Corporation
Mary Ann Davidson	Oracle Corporation
Peter Denning	Naval Postgraduate School
Ronald Dick	Computer Sciences Corporation
George Dinolt	Naval Postgraduate School (Facilitator)
David Dobbs	Northrop Grumman
Neal Donaghy	Georgia Tech
Thomas Donahue	Central Intelligence Agency
Thomans Dziuban	SRA International
John Edwards	Nortel Networks
Thomas Falvey	Department of Homeland Security/National Communications System
Leonard Ferrari	Naval Postgraduate School
Cristin Flynn Goodwin	BellSouth (Facilitator)
Peter Fonash	Department of Homeland Security/National Communications System
Gilberto Frederick	Department of Homeland Security/National Communications System
Deborah Frincke	Pacific Northwest National Laboratory
John Fulp	Naval Postgraduate School

Inette Furey	Department of Homeland Security/National Communications System
Kiesha Gebreyes	Department of Homeland Security/National Communications System
Seymour Goodman	Georgia Tech
Tim Grance	National Institute of Standards and Technology
John Grimes	Raytheon
Conrad Herrmann	Zone Labs
Chad Hinkle	Department of Homeland Security/National Cyber Security Division
Richard Houska	Georgia Tech
Richard Hovey	Federal Communications Commission
Robert Hughes	GuardedNet, Inc.
Cynthia Irvine	Naval Postgraduate School (Facilitator)
Michelle Keeney	U.S. Secret Service
Hank Kluepfel	Science Applications International Corporation
Eileen Kowalski	U.S. Secret Service
Paul Kozemchak	Defense Advanced Research Projects Agency
Marvin Langston	Science Applications International Corporation
Ben LaPointe	Motorola
Marc LeBlanc	Office of Science and Technology Policy
Sina Lehmkuhler	Department of Homeland Security/Science and Technology Directorate
David Liddle	U.S. Venture Partners
Steven Lines	Science Applications International Corporation
Jon Lofstedt	Qwest
Bert Lundy	Naval Postgraduate School
Susan Maraghy	Lockheed Martin Corporation
Gabriel Martinez	Department of Homeland Security/National Communications System
Maneck Master	Telcordia Technologies
Charles McQueary	Department of Homeland Security/Science and Technology Directorate
Ralph Merkle	Georgia Tech
Alan Michaels	Georgia Tech
Jeffrey Miller	Lab for Telecommunications Sciences
Delphine Nain	Georgia Tech
Peter Neumann	SRI International
Richard Pethia	CERT Coordination Center
Michael Petry	MCI
Janet Philpot	Carnegie Mellon University
Patricia Pichardo	Georgia Tech
Todd Pugh	Naval Postgraduate School
John Quarterman	InternetPerils, Inc.
Victor Raskin	Purdue University
Karl Rauscher	Lucent Technologies

Tiffany Reed	Department of Homeland Security/National Communications System
Evelyn Remaley Hasch	Booz Allen Hamilton
Scott Rickard	Authentium, Inc.
Robert Rosenstein	Carnegie Mellon University
Alberta Ross	Department of Homeland Security/National Communications System
Marek Rusinkiewicz	Telcordia Technologies
Richard Russell	Office of Science and Technology Policy
Anthony Rutkowski	VeriSign Inc.
William Ryan	Department of Homeland Security/National Communications System
Stratton Sclavos	VeriSign, Inc.
Chris Scholz	Georgia Electronic Design Center
William Semancik	National Security Agency
Tim Shimeall	Carnegie Mellon University
David Shinberg	Lucent Technologies
Ross Stapleton-Gray	Skaion Corporation
Victoria Stavridou-Coleman	Intel Corporation
DeJuan Stroman	Department of Homeland Security/National Communications System
David Su	National Institute of Standards and Technology
David Sulek	Booz Allen Hamilton
Gretchen Sund	Booz Allen Hamilton
Wim Sweldens	Lucent Technologies
Simon Szykman	Department of Homeland Security/Science and Technology Directorate
Victor Tambone	Department of Homeland Security/Science and Technology Directorate
Ted Tanner	Microsoft Corporation
Michael Tiddy	Lucent Technologies (Facilitator)
Louise Tucker	Telcordia Technologies
Pamela Warren	Nortel Networks
Jody Westby	PricewaterhouseCoopers LLC
Brian Witten	Symantec
Michael Yee	Defense Manpower Data Center

APPENDIX C: SPEAKERS’ REMARKS

Keynote Address
Mr. Richard M. Russell

Remarks by Mr. Russell, Associate Director for Technology, Office of Science and Technology Policy (OSTP), to the National Security Telecommunications Advisory Committee (NSTAC) Research and Development Exchange (RDX) Workshop, Monterey, California, October 28, 2004.

Thank you, Guy, for that kind introduction. I am pleased to be here with all of you today at the sixth meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) Research and Development Exchange (RDX) Workshop.

Since its creation by President Ronald Reagan in September 1982, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other national security and emergency preparedness (NS/EP) communications concerns. The RDX Workshop is an invaluable forum for information sharing between industry, Government, and academia.

Three years have passed since the attacks of September 11, 2001. And while the danger has not passed, America today is safer and stronger because of the actions taken by President Bush to protect our country. This Administration has taken unprecedented efforts to protect America's critical infrastructure against the threat of terrorism.

Already, the President has led the largest reorganization of government in more than 50 years; strengthened our intelligence capabilities; expanded support for first responders and state homeland security efforts; and increased the protection of our transportation systems, borders, ports, and critical infrastructure. NS/EP telecommunications has benefited from these efforts.

I would like to start by acknowledging the work of the NSTAC Next Generation Networks Task Force (NGNTF). The NGNTF was formed to study the impact of next generation networks on NS/EP communications. They have defined three critical areas and will:

1. Agree upon a high-level description of the expected network environment or ecosystem of next generation networks and its interdependencies;
2. Examine NS/EP user requirements, end-to-end user requirements, end-to-end services, and the interfaces and accountability among network participants and network layers; and,
3. Analyze relevant user scenarios and expected cyber threats.

Just a few weeks ago the NGNTF leadership was kind enough to provide OSTP with a
number of near term recommendations. The recommendations couldn't have come at a better time considering our heightened security concerns.

The NGNTF notes that networks are already converging to form the Next Generation Network. For example, service providers offering Internet protocol (IP) based telephony and high-speed Internet connections are now a mainstay of NS/EP communications.

Broadband availability is speeding this new era of IP based communications.

Earlier this year, President Bush announced support to expand access to high-speed Internet in every part of America. The President called for universal, affordable access for broadband technology by the year 2007 and wants to make sure we give Americans plenty of technology choices when it comes to purchasing broadband.

Broadband technology will enhance our Nation's economic competitiveness and will help improve the delivery of education and health care. Broadband provides Americans with high-speed Internet access connections that improve the Nation's economic productivity and offer life-enhancing applications, such as distance learning, remote medical diagnostics, and the ability to work from home more effectively. And it is important to note that broadband not only strengthens our economy, it also strengthens our NS/EP communications capabilities by providing new innovative means of communication.

The Bush Administration has implemented a wide range of policy directives to create economic incentives, remove regulatory barriers, and promote new technologies to help make broadband available. The Administration supports the Federal Communications Commission's (FCC) decision to free new fiber-to-the-home investments from legacy regulations. Deregulating new ultra-fast broadband infrastructure is working. Earlier this month some of the Nation's largest telecommunications companies announced that they plan to at least double the speed of their fiber rollout.

On Apri1 26, 2004, the President signed an Executive Memorandum that implements Federal rights-of-way reforms to streamline the process for broadband providers to get access to Federal lands to build high-speed infrastructure. The reforms will help to minimize burdens on industry by simplifying and standardizing the rights-of-way process across all relevant agencies, while allowing agencies to use their resources wisely.

Another example of expanded opportunities for NS/EP communications is in the area of Wireless Fidelity (WiFi) and Worldwide Interoperability for Microwave Access (WiMAX). The administration has made unprecedented strides in balancing the commercial spectrum needs of critical government agencies (including Department of Defense, Department of Transportation, and Department of Homeland Security) and commercial interests.

The Administration has identified, and is working to make available, a large block of both licensed and unlicensed spectrum for commercial applications. This spectrum will help speed the rollout of advanced wireless services such as Evolution Data Only (EvDO), existing wireless applications such as Wi-Fi, and new broadband technologies such as WiMAX. EvDO, Wi-Fi and WiMAX technologies can provide a range of new NS/EP services for Federal, State, and local officials.

All of these efforts are working. Broadband penetration has grown from seven million lines in December 2000 to twenty-eight million in December 2003. The FCC just opened the entire country to broadband over power lines. Intel just announced it is partnering to roll-out WiMAX.

I think we can all agree that the future is now and we need to begin an earnest effort toward better understanding the new threats and vulnerabilities presented by our new converged network environment. That is why this year's RDX Workshop is so important.

The theme for this year's Workshop is "A Year Later: R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness". The aim is to examine progress made since the last RDX Workshop and consider the new challenges we face. This morning I want to share with you a few of the success stories since the last RDX Workshop and present some of the ideas and plans we have for the future.

Let me start first with the overall Federal R&D budget...it is a good news story.

With the President's fiscal year (FY) 2005 budget, total R&D investment during this Administration's first term will be increased 44% to a record $132 billion in 2005, as compared to $91 billion in FY 2001. That equates to increases of nearly 10% each year, significantly outpacing the FY 2005 overall "non-security" discretionary spending growth of 0.5%.

Science and technology drive economic growth. They help improve our health care, enhance our quality of life, and play an important role in securing the homeland and winning the war on terrorism. These increases reflect the Administration's appreciation of the importance of a strong national R&D enterprise for our current and future prosperity.

The President's FY 2005 budget request commits 13.5% of total discretionary outlays to R&D, the highest level in 37 years. Not since 1968, during the Apollo program, have we seen an investment in research and development of this magnitude. Of this amount, the budget commits 5.7% of total discretionary outlays to non-defense R&D, the third highest level in 25 years.

Let me highlight a few examples of ongoing Federal communication R&D. I think it will showcase the importance of the work and the large number of agencies involved.

At the National Communications System (NCS):

> The NCS developed a route diversity methodology that enables federal agencies to rapidly and accurately evaluate their existing communications infrastructure. Route diversity is communications routing between two points over physically disparate paths.
>
> The NCS is continuing to develop and refine telecommunications dependency models to determine the impact of Internet disruptions on selected critical infrastructures.
>
> Over the past year, Wireless Priority Service (WPS) has grown from one nationwide Global System for Mobile Communications (GSM) carrier to four; from 3,000 users to over 11,000; and development has begun on Code Division Multiple Access (CDMA) platforms allowing Verizon Wireless and Sprint to join the existing GSM carriers in offering WPS by the end of 2005.

Technology insertion within the wireless industry continues at a rate that requires ongoing research and planning for migration of existing WPS capabilities to 3rd Generation (3G) communications technologies.

As the wireless world merges with 3G architectures, NCS is developing research and development programs to include:

- Development of specific Industry Requirements for inclusion of WPS functionality within Universal Mobile Telecommunications System (UMTS);
- Development of Next Generation Network prototypes supporting WPS capabilities with NS/EP Voice Over IP (VoIP) applications; and,
- Development of a wireless access framework for IP-based integrated voice and data NS/EP capabilities.

The NCS is also working on an effort that will lead to assuring current NS/EP services — such as Government Emergency Telecommunications Service (GETS), WPS, and others — are available in the next generation networks.

At the Department of Commerce (DOC):

DOC is conducting studies to develop tools that will improve the movement and communication of people within structures under emergency situations. They are also developing cyber security standards and guidelines.

At the Department of Defense (DOD):

DOD has created the capability to link real-time intelligence threat information with the identification of potentially threatened critical infrastructure.

They have delivered advances in the cyber arena in the critical realm of autonomous software agent technology including multi-agent system interoperability and cognitive agent architecture.

They are also working on unmanned sensors that perform ad-hoc networking for autonomous self-healing routing and that provide network security including authentication, data integrity, and privacy.

DOD is also developing realistic models of blast effects in urban and rural settings to forecast various impacts including limitations in movement of people and vehicles. This is particularly important to telecommunication restoration following a major incident.

At the Department of Energy (DOE):

DOE has established a Critical Infrastructure Test Range, which includes a multi-laboratory National Supervisory Control and Data Acquisition (SCADA) testbed to investigate cyber vulnerabilities and evaluate technologies to protect existing process control systems as well as security enhancements for new systems.

At the Department of Homeland Security (DHS):

DHS has produced an initial version of a fully integrated modeling, simulation and analysis system for use by national and regional leaders with decision support and planning capability across all 14 critical infrastructure sectors including telecommunications.

DHS has also completed an analysis of how to protect SCADA systems and is establishing a virtual National Cyber Security R&D Center.

At the Department of Justice (DOJ):

DOJ has completed a study on the real cost and consequences of insider threats. The study included multiple industries and the impacts and losses associated with this type of attack.

At the Department of Transportation (DOT):

DOT initiated Adaptive Quarantine research project to ensure that Federal Aviation Administration (FAA) is prepared to preempt active, passive, novel, insider and outsider cyber attacks against safety-critical and mission support networks and systems.

DOT is also proceeding with a renewed examination of the security and control of highways, bridges, tunnels and reducing the risk of the highway system being used as a means to deliver an attack. As so many of our nations telecommunications pathways follow public right of ways, this research is very useful.

Finally, at the National Science Foundation (NSF):

NSF has a variety of research projects that range from blast impacts to physical infrastructure models for systems and structures; applications of nano- and biotechnology in protective materials and devices; social dynamics of terrorism; cybertrust and cybersecurity; new architectures for secure and resilient cyber and physical infrastructure systems; integrated computational and information resource development; and sensor networks.

NSF is also investigating collaborative knowledge environments for the management of dynamic information, knowledge discovery; information extraction and fusion.

All these department and agency efforts, plus many others, directly or indirectly support NS/EP communications and the four aspects of trustworthiness (cyber security and software, human factors, physical security, and integration) that were raised at the last R&D Exchange Workshop.

I'd like to now share with you what we, within the Federal Government, believe to be the critical areas deserving special attention in the coming months and years.

The topics I am about to discuss were identified through the interagency R&D coordinating process under the President's National Science and Technology Council Infrastructure Subcommittee.

The topics are based on threat information and discussions with industry representatives, infrastructure owners and operators, and Government officials. We believe these nine areas will contribute to a stronger NS/EP posture for the Nation:

1. <u>Detection and sensor systems and related integration needs.</u> We must have the systems and tools to detect and sense what is occurring or even being planned or considered. We need to develop advanced detection and interconnected sensor systems for intuitive monitoring and rapid assessment of the condition of NS/EP communications and to identify approaching threats.

2. <u>Protection of assets and prevention of successful attacks against them.</u> We must have the systems, tools, methods and permissions to protect assets and NS/EP communications critical to the Nation. We need to develop effective protection of communication assets and prevent successful attacks against them with economically sustainable and operationally seamless measures.

3. <u>Security of entry portals and access to assets.</u> We must prevent unauthorized access to important places and systems. We need to develop smarter, more advanced security techniques for physical and cyber entry portals and access points.

4. <u>Insider threats.</u> We must address the dangerous situation of a trusted party who has passed all our controls, is inside our key assets and decides to betray that trust. We need to develop new methods to rapidly detect malicious behavior, track access to sensitive resources, and prevent actions damaging to NS/EP communications.

5. <u>Analysis and decision support systems.</u> We must have tools that can analyze complex and difficult problems and support our decision making in the most integrated and informed way possible. We need to develop analysis and decision support methods to provide a sound basis for setting infrastructure protection priorities.

6. <u>Response, recovery, and reconstitution.</u> If we do have a critical event, we need to be prepared to deal with the situation from initial response to final replacement of the lost asset or capability. We need to advance the response, recovery, and reconstitution capabilities for NS/EP physical and cyber networks, more rapidly restore the services they provide, and reconstitute the flow of communications.

7. <u>New and emerging threats and vulnerabilities.</u> We must recognize that there are new capabilities being developed by adversaries not previously considered or for which we may have insufficient knowledge and protection. We need to anticipate and target new

and emerging threats and deal with the new vulnerabilities that will be created as technology evolves and we shift emphasis and investments to higher levels of security.

8. <u>Advanced infrastructure architectures and system designs.</u> We must build new systems that do not have the faults or limitations of past systems and technologies that were created at a time when security was not as serious an issue. We need to provide advanced NS/EP physical and communication architectures and networked system designs that are inherently more secure.

9. <u>Human and social issues.</u> We must recognize the human assets are also elements of critical infrastructure. We need R&D on the best means to deal with the human-technology interface.

The areas I have described will likely require continuing work over many years. We also recognize that the results of research cannot simply be tossed over the wall with the hope that solutions will be automatically picked up by industry. We will need to work collaboratively to establish improved processes for technology transfer and diffusion of federally funded technology and intellectual property into commercial products and services.

Before closing, I would like to take a moment to express my sincere appreciation to the NSTAC for the many contributions it has made over the years to improve our national security posture. Your knowledge and expertise are invaluable to the President and the Nation.

A successful R&D agenda for NS/EP communications will require support, knowledge and contribution from almost every office in Government and from you. I appreciate your help.

I look forward to taking your questions.

Keynote Address: Dr. Charles E. McQueary

Remarks by Dr. McQueary, Under Secretary for Science and Technology (S&T), Department of Homeland Security (DHS), to the NSTAC RDX Workshop, Monterey, California, October 28, 2004.

I'm delighted to be here with you for the next couple of days and to witness firsthand the NSTAC RDX Workshop in action. In the terrorist threat environment that we have come to accept in our post 9/11 world, the work done by NSTAC and the research community that supports it has never been more timely or important. Your efforts to find solutions to the pressing challenge of ensuring trustworthy national security and emergency preparedness telecommunications is important to our national interests. The work that you do in the telecommunications sector informs decisionmakers at the highest level about national security.

I am impressed by the critical thinking that workshop participants are bringing to the table in identifying vulnerabilities and addressing the complex technical challenges we face….as we take the all-important step of elevating the nation to the next level of security to better protect our telecommunications infrastructure and its underpinning cyber infrastructure. Within the DHS S&T Directorate, we used the proceedings report from your previous RDX Workshop as one of the R&D reference documents during our recent five-year strategic planning cycle.

Robust telecom and information systems that are hardened and resilient in the face of an attack must be our future. And all of you here today are part of the effort, part of the momentum that is required to take us there.

I look forward to hearing from you during this RDX Workshop, and plan to share your views and findings with my colleagues at the Department of Homeland Security — so that we may be better informed in our own decisionmaking on these vital issues.

I want to begin by giving you a sense of where the Department's Science and Technology Directorate — my area of responsibility — fits into the overall framework of DHS. And beyond that, I want to give you an idea of the S&T landscape and where our telecommunications and cyber-related activities fit in.

Protecting the Nation by Air, Land & Sea

Our world today requires us to prepare for a series of brazen, surprise attacks that are calculated to take large numbers of lives and create economic harm.

In this country, we have 95,000 miles of shoreline, 7,500 miles of border, and 621 points of entry to protect. Every day, over 1 million people arrive at our airports and seaports. 2,500 airplanes and 600 ships bring them here, along with 2.5 million pieces of luggage. Another 320,000 passenger vehicles, 37,000 trucks and 20,000 containers enter the country daily. This translates to more than a billion transactions per year. And all we have to do is get it right every time.

This Administration supports a multi-layered approach to homeland security. If our enemies successfully penetrate one layer of security, they are confronted with several other protective layers that increase the likelihood of thwarting or diminishing the impact of a terrorist strike. We join with our many partners in homeland security — with those in industry, academia, and at all levels of Government — to do everything in our collective power to prevent another large-scale attack. At the same time, we know we must also be prepared to respond decisively and effectively to limit the consequences of an attack, should one occur, and save lives.

While our primary focus at the Department is one of protecting the American people from terrorism, DHS has an all-hazards mission. Many of the systems that we put into place for emergency preparedness and response were designed with a dual purpose in mind — and are pressed into service to prepare for, protect against and respond to major incidents unrelated to terrorism and natural disasters — such as earthquakes and hurricanes.

Key operational units of Homeland Security play crucial roles in preventing a major attack in this country — and in response and recovery operations, in the event of an attack. They are responsible for border and transportation security; emergency preparedness and response; intelligence gathering and critical infrastructure protection; and science and technology applications for homeland protection. The Coast Guard and Secret Service also play an important role here.

The Science & Technology directorate provides vital support to the other DHS operational units. Many of you have worked with or are otherwise familiar with the Department's Information Analysis and Infrastructure Protection (IAIP) directorate. IAIP is the center of the Department's intelligence analysis and infrastructure protection operations — and is responsible for preparing the annual National Infrastructure Protection Plan.

S&T supports IAIP by researching and developing new tools and technologies to improve the security of all of the critical infrastructures. We collaborate with the NCS and the Department's National Cyber Security Division — both are divisions of IAIP — on R&D efforts that fall within the scope of this Exchange Workshop.

S&T and Infrastructure Protection

DHS Science and Technology mobilizes the intellectual capital of the engineering and scientific communities to develop fresh and effective approaches to homeland protection. Our mission is to apply the nation's research, development, testing and evaluation capabilities to develop the technologies and solutions needed to defend against the methods and tactics of terrorists. The second part of our mission is to get these capabilities into the hands of emergency responders, critical infrastructure owners and operators, and others on the front lines of homeland defense.

Toward this end, S&T looks to:

- Detect, prevent and mitigate chemical, biological, radiological/nuclear and high explosives (CBRNE) threats;
- Assess and analyze threats and vulnerabilities;

- Provide technical solutions to federal, state and local emergency responders; and,
- Secure the nation's borders and critical infrastructure.

S&T identifies and integrates information from many sources with the expert evaluation and judgment of our scientific staff in determining and prioritizing the requirements of our R&D mission.

I should also mention that although the 9/11 Commission Report outlines no specific tasks for S&T, we are taking the report and its recommendations into consideration as we plan activities that support DHS components and our other partners in homeland security.

The directives, recommendations and other inputs that help to shape our R&D agenda include:

- Homeland Security Act of 2002;
- The FY 2005 Congressional Appropriations for DHS;
- Current threat assessments as understood by the Intelligence Community;
- President Bush's National Strategy for Homeland Security and numerous sub-strategies that include the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets and the National Strategy to Secure Cyberspace; and
- The President's 12 Homeland Security Presidential Directives (HSPD).

HSPD 7 — Critical Infrastructure Identification, Prioritization, and Protection — designates DHS as the federal lead for protecting information technology and telecommunications infrastructure as well as other critical infrastructure. This directive is an important driver of S&T's work in these areas.

Requirements of this Presidential Directive that S&T is addressing include:

- Interagency coordination [with the Office of Science and Technology Policy] on R&D to enhance protection of critical infrastructure and key resources;
- Private sector collaboration for sharing information about physical and cyber threats, vulnerabilities, incidents and best practices;
- Comprehensive modeling of the potential implications of terrorist attacks on critical infrastructure and key resources, especially in densely populated areas; and,
- Establishing an organization to serve as a focal point for cyber space security – the now well-known National Cyber Security Division.

S&T is ramping up R&D activities aimed at improving the security of information technology (IT), telecom and other critical infrastructures this fiscal year, and is actively leading interagency R&D coordination activities in the areas of critical infrastructure protection and cyber security.

The steps we take to enhance the security of our telecommunications infrastructure, pay dividends by strengthening the integrity of the many critical infrastructures that depend upon it — providing an important layer of protection for the nation.

The four key offices of S&T have an important role in implementing S&T's research, development, test and evaluation activities. These offices focus on:

- Science and technology planning and budgeting;
- Research and development;
- Advanced research through the Homeland Security Advanced Research Projects Agency — known as HSARPA; and,
- Systems engineering and development.

Three of these offices — Research & Development, HSARPA, and Systems Engineering & Development — are funding mechanisms for the R&D activities of the Department.

The fourth S&T office — Programs, Plans and Budgets — provides the strategic and technical vision for S&T and its research, development, test and evaluation process. This vision is implemented through many S&T portfolios. We have portfolios that address the major CBRNE threats — chemical, biological, radiological/nuclear and high explosives. S&T's emerging threats, rapid prototyping, standards and university portfolios crosscut or inter-weave with the CBRNE portfolios and with others that support DHS directorates, the Coast Guard and the Secret Service. Our Critical Infrastructure Protection (CIP) and Cyber Security portfolios are part of this group and serve as the S&T research liaisons to the infrastructure protection organizations within the IAIP directorate. IAIP is tasked with identifying and assessing the nation's vulnerabilities in critical infrastructures and the CIP and Cyber Security portfolios collaborate with this directorate on identifying R&D requirements for these areas.

Crisis Decisionmaking

The CIP portfolio — in collaboration with the NCS and Argonne, Sandia, Los Alamos and Pacific Northwest National Labs — is developing a decision support system that revolves around all 14 critical infrastructures and key assets identified in the *National Strategy for Homeland Security*. This effort maps out the types of threats and potential means of attacks against the critical infrastructures, and pays particular attention to their complex interdependencies. It incorporates threat and vulnerability assessments, and analyses that are based on comprehensive advanced modeling and simulation. This system will be used by Federal, State, and local governments as well as industry decision makers to prioritize protection, mitigation, response, and recovery strategies to help them plan for the consequences of a terrorist attack against our critical infrastructures. It will also support red-team exercises and provide real-time support during crises.

The value of the CIP/Decision Support System tool is that it fuses a wide variety of disparate information into a well-conceived modeling framework to support governors, mayors, chief executive officers, and decisionmakers at the federal level who must act quickly and smartly to minimize the consequences of an attack.

Working with the national labs and other partners, S&T used the decision support tool to simulate physical attacks on three telecom sites in metropolitan areas and observe the impact on all the other critical areas. The results showed that such a scenario would have a cascading effect and significantly disrupt sectors that include energy, Government, postal and shipping, food, water, public health, emergency services, transportation — and financial services, the sector that would bear the greatest impact. Outcomes include banks becoming disconnected from their networks as well as interruptions in ATM service, credit card and wire transactions, and check clearing operations. Financial losses would escalate during the anticipated 30-day recovery period, due to physical damage near affected facilities and telecom and power service interruptions. Losses would be expected to approach $600 million in one month.

This Decision Support System tool continues to evolve and has not been fully tested. However, it has successfully been pressed into service to inform security planning for National Special Security Events such as the conventions in New York and Boston last summer, and at other times of high alert.

S&T is coordinating with the IAIP Sector Coordinating Councils to improve and advance this modeling tool. And we will work with all levels of Government, and with infrastructure owners and operators, to improve sector models, validate simulations, and analyze cross sector interdependencies among all of the nation's critical infrastructures.

Cyber Security

We know that the nation's cyber assets are vulnerable to the potential for costly and highly disruptive cyber attacks. Cyberspace provides the opportunity to exploit weaknesses in our critical infrastructures and it may also provide a base for leveraging physical attacks.

S&T, through our Cyber Security portfolio, and the National Science Foundation are collaboratively funding a large-scale test bed for next generation information security technologies for cyber defense. Now underway, this effort will develop and use a physical network test bed and a software-testing framework to test attack and defense methods. It will enhance understanding of cyber security issues and requirements by integrating analytic methods and experimentation on a large-scale network. This program is expected to grow into a larger-scale test bed environment that is expected to be fully operational in 2006. In the future, we expect to integrate this test bed with others developed by DHS or perhaps the national labs or private sector. We expect these integration efforts to begin sometime after 2006. The test bed program is just one of several cyber security R&D programs underway within S&T.

Crisis Communications & Response

On 9/11, we know that lives were lost due to widespread communications problems. An integrated, national communications system — that can function at all levels of Government during an emergency — must be at the core of our disaster planning efforts.

Toward that end S&T has established an Office of Interoperability and Compatibility to coordinate activities in public safety communications, equipment and in the training of emergency responders.

One major federal effort underway will establish a common standard for interoperable wireless communications. This will help 44,000 local, tribal and state entities and 100 federal agencies engaged in public safety to communicate effectively with one another — particularly during an emergency.

Other plans call for using computer-driven devices to facilitate interoperability and link radio, cellular and landline phones at pilot sites. We also plan to set standards to foster compatibility in equipment for first responders across multiple jurisdictions. Yet another focus will be on standardized training for all first responders so they can affect a timely, efficient response that may save lives during a crisis.

As part of this effort, S&T successfully completed its initial phase of RapidCom — a focused Government campaign to boost interoperability in communications and facilitate a quick response to major incidents in 10 urban areas.

Funding to Fight Terrorism

Funding of homeland security initiatives to fight terrorism in the U.S. has increased substantially. From FY 2002 to FY 2004, this Administration has allocated $13.1 billion for first responder and public health terrorism preparedness — an increase of over 920 percent over the $1.2 billion spent in the previous three fiscal years. This figure includes funding through the Department of Justice, the Department of Health and Human Services, and the Department of Homeland Security.

- The Department of Homeland Security's budget has increased from $19.8 billion in 2001 to $40.7 billion in the Department of Homeland Security Appropriations Act of 2005, signed by the President last week.
- This includes $1.1 billion for S&T, an increase of over $200 million from the 2004 funding level.
- Since March of 2003, DHS has allocated and awarded more than $8 billion in overall grant funding to states and territories to support first responders and enhance the security of urban areas and their mass transit systems and ports.
- Here in California, the Department has allocated $805 million in funds for emergency preparedness and enhanced preventive and protective measures with an emphasis on urban, transit and port security.

I thought I'd wrap up my remarks on a historical note. Yesterday marked the 100th anniversary of the opening of the New York City subway. There was tremendous anticipation and excitement about America's first subway and 150,000 New Yorkers were on hand to try it out on opening day. The introduction of the new underground transit system seemed to mesmerize even the most jaded New Yorkers of the day. The October 28, 1904, edition of the *New York Times* described it this way:

'The general public would not be admitted until 7 o'clock, and its curiosity was vastly whetted all the afternoon by the unfamiliar appearance of crowds emerging from the earth. Of this sight, New York seemed never to tire, and no matter how often it was seen, there was always the shock of the unaccustomed about it. All the afternoon the crowds hung around the curious-looking little stations, waiting for heads and shoulders to appear at their feet and grow into bodies. Much as the subway has been talked about, New York was not prepared for this scene and did not seem able to grow used to it.'

Those were the days, when adults and children alike could be entertained by watching people emerge from a subway station. One hundred years later, subway systems are critical to the transportation infrastructure of New York City and numerous metropolitan areas across the country. Like anything else that draws large crowds — they are an attractive target for terrorists and must be protected. We know our transportation and telecom infrastructures have interdependencies and that a physical attack against one will disrupt the other, with likely impacts to additional infrastructures. Our modeling research will give us the ability to quantify these impacts as they may cascade across all the critical infrastructure sectors.

S&T has deployed a program called PROTECT that is designed to detect and respond to chemical agent releases in mass transit and other public facilities and spaces. In the event of a chemical attack, PROTECT triggers an early warning crisis management response that may halt the trains, shut off ventilation systems, facilitate evacuation — and provide situational awareness to responders who are off site.

PROTECT currently provides important safeguards for 1.3 million subway passengers who ride the Washington, DC and Boston area trains during the average workday. As the program expands nationally, it could protect an estimated 8.8 million subway riders each weekday. PROTECT is one of many promising technologies that will help safeguard large numbers of Americans.

The Department, S&T, and our many partners in homeland security in the public and private sectors continue to work on solutions to keep our citizens safe from the reach of terrorists. We are making good progress but we know that we have a lot more work to do.

Science and technology, driven by American ingenuity, is providing us with the tools to protect against, detect, and respond to terrorist threats against our nation. And our enemies should never underestimate the heart and spirit of the American people. We have shown the world that we have tremendous resiliency in the face of an attack. And that will take us a long way in our efforts to defeat terrorism.

In closing, I'd like to commend NSTAC and the RDX Workshop participants for your valuable contributions to safeguarding the nation's critical telecommunications and cyber infrastructures. I look forward to hearing the results of your breakout sessions that will take place today and tomorrow. Thank you for your time.

Luncheon Address
Mr. F. Duane Ackerman

Putting Our Brains Together: 21st Century Security Depends on 21st Century Partnership

Remarks by Mr. Ackerman, Chairman and Chief Executive Officer, BellSouth Corporation and Chair of the President's NSTAC, to the NSTAC RDX Workshop, Monterey, California, October 28, 2004.

Thank you, Pete…Good afternoon. Just a few minutes from here are the grounds of the Naval Postgraduate School. It is appropriate that our 6th RDX Workshop should be held here, not only because the School is partnering with NSTAC in hosting this event, but also because this month marks the 229th birthday of the United States Navy.

The Navy has built the finest fighting force in the world. Their history is America's history and it's one of innovation. It could have been otherwise. I don't know if this is a true story, but I heard that a delegation of representatives from various scientific groups went to Washington when the United States entered World War I to formally offer their services to the U.S. Navy. The delegation was politely received…heard… and asked to return the next day for an answer. They did so, and were told, 'No, thank you. The Navy already has a scientist.'

Fortunately, the scientists eventually won that battle and today, the professors and students at the Naval Postgraduate School embody a fundamental American idea: that we can advance the cause of human freedom, security and prosperity through science and technology. We are a nation that believes our greatest strength comes not from our firepower but our brainpower.

At the dedication of the School in 1952, a rear admiral said the following: 'Let us not become so hypnotized by the problems of production of hardware that we fail to recognize the problem of creation of brains capable of ensuring that hardware is indeed useful, and that proper use is indeed made of it.' I was struck by those words because they reminded me of something I said when we met at last year's RDX Workshop. And that was…our most important challenge in ensuring trusted networks was to close the gap between the pace of technology and our ability to manage it across industry and Government.

A year later, I believe more than ever that 21st century security depends on 21st century partnerships. If I may draw on the words of the rear admiral: The real test before us may not be whether we can put hardware…chips and circuits…together, but whether we can put our brains together. Over the past year, the members of NSTAC have done just that together with our Government and research partners. I want to acknowledge three of our Government partners in particular…all formidable brains, indeed.

Pete Fonash, I appreciate your leadership at the NCS, in particular, your support of that model of public-private partnership, the National Coordinating Center for Telecommunications (NCC). I also want to recognize Richard Russell, from the Office of Science and Technology Policy and Dr. Charles McQueary from the Department of Homeland Security. Thank you, gentlemen, for joining us and for being such strong technology advocates at the national policy level. I want to thank the RDX Workshop participants for the work you have accomplished and the work you are about to do today.

One of the issues you identified last year was 'a strong sense of frustration and urgency' in driving change in how we manage trustworthiness across Government, industry and academia. Thanks to your work, I think we have built a common agenda of urgency, partnership, and trust. Today I want to ask us to continue on that journey. As you head into the breakout sessions, I'd like to highlight four opportunities for putting our brains together.

Four Opportunities for Putting our Brains Together

In the past year we have seen a significant rise in the interdependencies of our critical infrastructures. If I had to sum up the last year in a few words, I'd probably say it was the 'year of Hurricanes and Hackers.' And just as the public switched telephone network is converging with next generation networks, physical security is converging with cyber security.

Here's the first question I want to raise: as we accelerate the move to fiber and digital network technologies, how do we manage the increasing interdependencies across our physical infrastructures?

Mother Nature asserted herself and reminded us that we can't get complacent about physical security. BellSouth's region was hit by the worst hurricane season in over a century. Four hurricanes in six weeks… Before one storm could make landfall, another would brew, churning up winds and rain. As each finally came ashore, it cut a wide path of destruction. In terms of our physical plant, we had some 19,877 cable spans and 6,584 poles destroyed.

To restore service we deployed massive amounts of equipment and resources – 1,100 generators were deployed multiple times and 540,000 gallons of diesel fuel kept central offices running. Overall our recovery efforts were strong. We did not have a single central office fail and our technicians were able to restore service to most of our customers quickly.

One of the lessons that stood out during this hurricane season is telecommunication's increasing interdependence with other sectors of critical infrastructure. BellSouth had more than two million access lines affected by a loss of commercial power. That's not a huge number given the 22 million lines we have overall, but this will become a bigger issue as we continue the move to fiber and digital networks that, unlike copper lines, depend on commercial power.

Customers will also be more vulnerable as they migrate to communications services provide by all providers as applications over broadband networks. During Hurricane Frances, for example, Adelphia and Comcast said 33 to 80 percent of their subscribers lost service because of power outages. The two million plus BellSouth lines that were affected by commercial power loss included some 319,664 digital subscriber lines (DSL) lines. It's becoming very clear that with the shift to IP services, there is a shift in responsibility to the end-user.

In the old wireline world, customers knew when they picked up the phone they would get that dial tone because the phone company would take care of it. We actually "trickled" power to the premise over our physical connections to provide dial tone even when commercial power failed. Now, end-users have to be more involved in managing their communications services.

In the future, back up generators cannot be the primary answer when large-scale disasters strike. We need more R&D around alternative emergency power technologies. But resiliency will also depend on educating end-users about the implications of new services as well as our ability to partner across critical infrastructures.

Second question: as we shift to next generation networks, how do we capture the benefits of broadband and yet, with clear eyes, plan to deal with its security implications?

This was not only the year of hurricanes. It was also the year of hackers who have become increasingly sophisticated in exploiting the convergence of the public switched telephone network with the Internet.

As an industry, we are rapidly shifting toward broadband delivery of communications services over a wide range of devices. Converging all of these edge devices is Internet Protocol. New technology is delivering more benefits to customers. It expands our choices, but also make us more vulnerable.

What traditionally was a more closed, secure environment is now more open. And, our security depends not only on the two billion miles of physical circuits, but also the integrity and configuration of software and hardware. A survey of Internet vulnerabilities released last month showed a sharp jump in attacks on personal computers during the first six months of this year, with an average of 48 new vulnerabilities a week. Worms and viruses had increased four and a half times since last year. The Internet con known as "phishing" has skyrocketed by almost 500 percent this year. Hackers can take over computers from anywhere in the world. You don't know where the attack originated. You may not even know you are being attacked or that your PC is a tool in someone else's attack.

As the public switched network converges with the Internet, we are exposed to new threats through billions of access points. But we also have new opportunities. One answer is to see broadband technology not just as a security challenge, but as a security solution.

In protecting citizens, Government agencies communicate urgent and life-saving information. A trusted computing environment will encourage Americans to take advantage of broadband and its power to deliver rich information faster. Through NSTAC we can promote the development of technology that will increase the security of a citizen's online experience.

Think also about the opportunities around applications that can help in the defense of our nation. The Government's ability to collect, analyze, and visually represent data – perhaps, in real time – will require applications that run over high-speed, robust and secure networks. One example would be remote monitoring of infrastructure over instrumentation such as SCADA systems or video. Remote sensors can be used to detect radiation or transmit data from bio-surveillance systems.

Secretary Ridge has talked about the possibility of first responders sending live video feeds from a helmet-mounted camera back to a central command position, whether they're in the middle of a storm or responding to a terrorist attack. Fiber and broadband deployments should bring costs down, so these types of solutions can be applied across a much wider scope. Greater broadband access in more locations can decrease the concentration of resources at single sites, making them less vulnerable targets.

Secretary Ridge has pointed out that America "built an arsenal of democracy to win World War II." I believe that today broadband is an indispensable tool in our arsenal of democracy. But as we build our broadband tools, let' s not be in denial about the change in our security profile and the need to address it. If we address it, if we do it right and make it more secure, it will take capital.

Third, assuming we have put the standards and expectations in place to create a secure system, what is the role of public policy in encouraging investment in secure next generation technology?

I am encouraged by the recent FCC decisions to clear out some of the regulatory underbrush. I am pleased that old rules intended for traditional telephone networks won't be applied to new broadband and IP networks. And as a result of this little breeze of clarity, there have been several announcements of accelerated fiber deployment. This is good news for Americans, especially in light of a recent report that says the U.S. has dropped to 13th among broadband users worldwide.

But even with the recent decisions, too much uncertainty still lingers over fiber and packet deployment. The 1996 Telecommunications Act was written for another age, before broadband and the Internet. And the role of state regulation has not yet been clarified. Meanwhile, technology is out-pacing even the shortest policy cycles. The President has said: "Science and technology have never been more essential to the defense of the nation and the health of the economy." With Asian economies on the rise and with the war on terror, can America afford to settle for 13th place?

In the 20th century, America lived up to its promise as a prosperous and peaceful nation, in part, because of our advanced communications infrastructure. That promise is still there, if we can create rules that make economic sense. Let's work toward policy that is pro-technology, pro-security and pro-investment.

I have a fourth question. This is really the question that all others hinge on, and it has to do with partnership. Quite simply, how do we remove the barriers that keep us from putting our brains together?

In making our country more secure, we have to overcome major cultural, competitive, and regulatory barriers that impede information sharing and cooperation. The 9/11 Commission's report made that point very well. And while the report focused on Government, I think it has lessons for all who own and operate our nation's critical infrastructure. Calling for unity of effort, the Commission noted that the U.S. Government has access to a vast amount of information. But it has a weak system for processing and using what it has. The Commission recommended that we change from a system of "need to know" to one of "need to share."

The good news is we have several foundations for partnership in place. Through NSTAC, we have made progress in balancing openness with competitiveness. We are identifying vulnerabilities in how we manage critical infrastructures. We are building common definitions. On the issue of trusted access, we've begun to develop criteria for how industry and Government can work together on national background checks.

Working with organizations like the Alliance for Telecommunications Industry Solutions (ATIS) and Banking Industry Technology Secretariat (BITS), we have made progress in the financial services sector, on developing standards and in mapping out some of the many interdependencies across industries. We are also coordinating our work on next generation networks with other parts of the industry to ensure we are giving the best advice possible to the President of the United States.

One of our best models for public private partnership is the NCC, which is located in the Department of Homeland Security. Through the NCC, industry and Government have worked together to plan for and respond to natural and man-made disasters. We shared resources and response capabilities following 9/11, and have provided full-time employees to the Department of Homeland Security. The NCC is a success story. And that's why NSTAC members are firmly committed to working with the NCC and the National Communications System in the future because we believe it's one of the most effective partnerships we have in place today.

You know, hurricanes don't care whether they take out a power line or a phone line. Hackers don't care whose computer they take over, to them it's just one vast cyberspace. Terrorists don't care whether their targets are telecom providers or software providers or energy providers. They don't care whether we're Government or industry. They simply want to hurt America. And they will exploit our divisions and weaknesses.

In the days following 9/11, I said to employees at BellSouth that our most powerful act, our one true triumph over this tragedy, was our unity as a company and a nation. Three years after 9/11 as American service men and women are defending our nation at home and abroad let me say that our most powerful act is our unity as the stewards of our nation's infrastructure.

Today I want to ask us to turn our agenda of urgency, partnership and trust into action. Let's see reality with clear eyes. Let's be creative. Let's be determined. And let's keep doing the hard work of putting our brains together to keep America secure and strong.

I look forward to the results of your work.

Thank you.

APPENDIX D: 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 Chairman of the National Council on Competitiveness, Chairman of the National Security Telecommunications Advisory Committee (NSTAC), member of the Homeland Security Advisory Council, 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.

John Arquilla is an Associate Professor of defense analysis at the Naval Postgraduate School (NPS). He joined the faculty in 1993 as an Assistant Professor of National Security Affairs. Dr. Arquilla is also a Senior Consultant at the RAND Corporation.

Dr. Arquilla earned his degrees in international relations from Rosary College (BA, 1975) and Stanford University (MA, 1989; PhD, 1991). His research and teaching interests include information-age conflict, revolution in military affairs, and irregular warfare. Applications of this research have included attack and defense of critical infrastructure, delaying large industrial projects or weapons programs, theater ballistic missile defense, sensor mix and deployment, communications network diversion, underground mining, and semiconductor manufacturing.

Dr. Arquilla maintains a variety of professional affiliations, from founding membership in the Highlands Forum (a government-industry-academic consortium concentrating on issues in information technology), to his role as senior consultant to the International Security Group at RAND. His work on the security implications of the information revolution has formed a basis for analysis of these issues in academia, industry and Government. His ideas have also reached broad general audiences in publications including; *Time, The Economist, The New Republic, Wired, The New York Times, Le Monde*, and *Al-Hayat.*

David Barron is currently serving as Assistant Vice President for BellSouth Corporation in the Washington, D.C. office. He is responsible for National Security matters for BellSouth in its relationship with the Federal Government. In this role, Mr. Barron directly supports F. Duane Ackerman, Chairman and CEO of BellSouth, while Mr. Ackerman serves as Chairman of the NSTAC, a Federal Advisory Committee consisting of Presidential appointees.

Mr. Barron is the Working Session Chair of the Industry Executive Committee (IES), the working committee that supports NSTAC. He also serves as the Vice Chairman of the NSTAC Outreach Task Force and serves on the Legislative & Regulatory Task Force and on the Research and Development Task Force. He is also a member of the BellSouth Corporate Security Council and works with numerous

Federal Executive agencies on issues of National Security, Homeland Security and Emergency Preparedness. He also serves on the United States Telecommunications Association National Security Policy Committee and attends the Federal Communications Commission's (FCC) National Reliability and Interoperability Council. Mr. Barron also has responsibilities for Congressional Relations with the Louisiana and Mississippi delegations plus other Congressional delegations that are assigned work on national security matters.

Prior to his Washington assignment, Mr. Barron was Director-Regulatory in New Orleans, Louisiana. In this capacity, he was responsible for interfacing with the Louisiana Public Service Commission on policy issues, customer service, rate and tariff matters and external affairs involving the Commission. Mr. Barron also has occasion to work with various Louisiana State Government agencies and the FCC on issues involving BellSouth. Mr. Barron is a graduate of the University of Mississippi with a BBA in Management and a graduate of the Louisiana State University Executive Management Program.

Frank Cantarelli is a Sr. Technical Manager at Lucent Technologies. In this role, Mr. Cantarelli is in charge of developing Network Solutions to meet Lucent's Government Customers' requirements. Mr. Cantarelli began his career as a Field Engineer at IBM in 1984, and has spent 20 years in system deployment, development, marketing and sales of communication systems, with Hughes Aircraft, Lockheed Martin and Qwest Communications.

Mr. Cantarelli holds a bachelor's degree in Electrical Engineering from The University of Illinois, a master's degree in Business Administration from Marymount University and a master's degree in Electrical Engineering From George Washington University.

Matthew Carlyle is an Associate Professor in the Operations Research Department at NPS. He joined the faculty in 2002 after five years as an Assistant Professor in the Department of Industrial Engineering at Arizona State University.

Dr. Carlyle received his Ph.D. in Operations Research from Stanford University in 1997, and his B.S. in Information and Computer Science from Georgia Tech in 1992. His research and teaching interests include network optimization, integer programming, and network interdiction. Applications of this research have included attack and defense of critical infrastructure, delaying large industrial projects or weapons programs, theater ballistic missile defense, sensor mix and deployment, communications network diversion, underground mining, and semiconductor manufacturing.

Guy Copeland is Vice President, Information Infrastructure Advisory Programs, with Computer Sciences Corporation (CSC), Federal Sector. He represents CSC's CEO, Van Honeycutt, in the President's NSTAC, a body that provides industry advice to the President of the United States, regarding critical information and telecommunications services supporting our national economy and other critical functions of society. Mr. Honeycutt chaired the NSTAC from September 1998, to September 2000. During that period Mr. Copeland served as the chair of the working body of the NSTAC, the Industry Executive Subcommittee Working Session. He currently chairs the Research and Development Task Force of the NSTAC. He joined CSC in January 1988 and served progressively as Director of Program Management Operations, Director of Implementation and Deputy Project Manager for the Treasury Consolidated Data Network, and Director, Network Integration Division Engineering Center.

In the early 1990's, Mr. Copeland championed an NSTAC initiative that was a progenitor for the information sharing and analysis center (ISAC) concept. Later he served as Chair for three groundbreaking NSTAC collaborative inter-sector risk assessments. He now serves as CSC's member on the Board of Directors of the Information Technology ISAC where he was elected Vice President. 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. He was Co-Chair of the Early Warning Task Force begun at the National Cyber Security Summit for DHS in December 2003. Mr. Copeland Chaired the Armed Forces Communications Electronics Association (AFCEA) symposium on critical infrastructure protection in 1998, 1999 and 2000.

Mr. Copeland represented CSC for three years on the board of the Corporation for Open Systems International. He served as organizing chair for the first Asynchronous Transfer Mode Workshop for the Communications Society of the Institute of Electrical and Electronic Engineers (IEEE) in 1995 and was overall co-chair for the 1996 workshop. He served as a member of the initial advisory board for "IT Professional," a new publication of the Computer Society of the IEEE. 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. He serves on an advisory committee to a U.S. Secret Service research project on the threat posed by those with inside access to computers and networks.

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 (while still a U.S. resident, Canadian citizen); and Military Assistant to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) for the Joint Tactical Information Distribution System (JTIDS). He represented the United States in negotiating an eight-nation agreement for a cooperative program to develop a North Atlantic Treaty Organization version of JTIDS.

Mr. Copeland serves on the Executive Programs Advisory Panel of the University of Maryland, University College. He is a Senior Member of the IEEE. From 1983–1984, 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. His other memberships include Eta Kappa Nu (Electrical Engineering Honor Society), Tau Beta Pi (Engineering Honor Society), the Army Aviation Association of America, the Association of the United States Army, and the Information Systems Security Association. His degrees are: M.S. Electrical Engineering, University of California, Berkeley; B.S. Electrical Engineering, University of Wisconsin, Madison.

George Dinolt joined the NPS faculty in the Computer Science Department in January 2002 as an Associate Professor. From 1982-2000 he worked as a Technical Consultant for Research and Advanced Programs in Computer Security and Special Projects at Ford Aerospace, Loral and Lockheed Martin Western Region. Prior to that, Dr. Dinolt worked as a Senior Engineer in the Engineering Computer Center of Car Engineering at Ford Motor Company. From 1971-1977 he taught and conducted research as an Associate Professor in the Mathematics Department of the University of Michigan at Dearborn. His teaching interests include formal methods, computer security, computer security systems architecture and other special projects.

Dr. Dinolt received his BA in Mathematics from Lawrence College in 1964. Shortly thereafter, he completed his MA in Mathematics at Wake Forest College. In 1971, Professor Dinolt earned his PhD, also in Mathematics, at the University of Wisconsin, Madison.

Cristin Flynn Goodwin is BellSouth's Director of Homeland Security and Strategic Policy. Ms. Flynn Goodwin represents BellSouth at the National Communications System and National Coordination Center on policy issues, and handles the Company's Crisis Coordination and Disaster Response needs at the Federal level. Ms. Flynn Goodwin oversees the internal BellSouth team responsible for Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service.

Ms. Flynn Goodwin represents BellSouth on issues related to critical infrastructure protection, homeland security, standards development, and physical or cyber-security issues. She also participates in a number of industry groups, including the President's NSTAC, where she recently served as the Vice-Chair of the Financial Services Task Force, and the Chair of the United States Internet Service Provider Association's Cyber Security Working Group. Ms. Flynn Goodwin is also an attorney, and she is actively involved in many of the legal issues and concerns surrounding today's homeland security and infrastructure protection discussions.

Cynthia Irvine is a Professor of Computer Science, Director of the Institute for Information Sciences and Operations, and Director of the NPS Center for Information Systems Security Studies and Research (CISR). Through her efforts NPS CISR is one of only fourteen nationally recognized Centers of Excellence in Information Assurance Education.

In 1994, Professor Irvine rejoined the academic faculty of the Department of Computer Science at the Naval Postgraduate School after working at Gemini Computers, Inc. on the development of high assurance, secure computer systems. She has a joint appointment in the Department of Electrical and Computer Engineering and participates in the Information Warfare and Modeling, Virtual Environments and Simulation Academic Groups. At NPS she has taught courses in introductory and advanced computer security, algorithms, distributed systems, software architectures, network security, modeling and formal methods, and secure systems. She has also worked to create a sequence in Information Assurance and computer and network security that ranges from introductory to advanced topics.

Dr. Irvine has contributed to computer security education at NPS by developing a laboratory that supports both teaching and research. Professor Irvine's research is on issues of information assurance, with a secondary interest in the safety and reliability of computer systems. Her work in high confidence security policy enforcement and multilevel security has resulted in cited papers in the principal computer security literature.

In 1996 Dr. Irvine founded NPS CISR, of which she is the Director. In the area of research and development for high assurance computer security, NPS CISR boasts the largest and most experienced academic research group in the world. Dr. Irvine's research focuses on architectures and design of secure distributed systems that must protect both high sensitivity and high reliability data, such as state secrets or information upon which critical decisions must be based. Dr. Irvine also conducts research on issues relating to increasing the ability of emerging adaptive systems to take advantage of security choices. This has resulted in the first distributed ring architecture for a resource management system and the first model for quality of security service.

In 1999 Dr. Irvine took over the lead of a large project funded by the Defense Advanced Research Projects Agency (DARPA) on resource management systems. This effort involves researchers at three universities and in industry and has resulted in fundamental contributions in the area of the use of heuristic techniques to choose algorithms for resource management systems and in security for these systems. In 1999, the Director of DARPA appointed her to the Information Security Research Council Science and Technology Study Group on the future of research in information assurance. Dr. Irvine also leads an NPS-based effort to develop a version of the Linux operating system that will have the functional characteristics of a label enforcing secure system.

Dr. Irvine is currently Chair of the Sub-Committee on Academic Affairs of the Technical Committee on Security and Privacy of the IEEE. She is Secretary of the ACM Special Interest Group on Security and Audit Control. She is a member of the Board of the National Colloquium on Information Systems Security Education. Dr. Irvine is a member the International Federation for Information Processing Technical Committee 11 Working Group 11.8 on Information Security Education and Training. She is a member of the Computer Society of the IEEE. She is also a member of the Usenix Association. Dr. Irvine founded and chaired the Workshop on Computer Security Education, which has been held annually since 1997.

Dr. Irvine received her BA degree with a major in Physics from Rice University, Houston, Texas. She then attended the Case Western Reserve University in Cleveland, OH where she held a National Defense Education Act Fellowship to study Astronomy. Upon receiving her PhD in Astronomy she joined the emerging Computer Science Group at the Naval Postgraduate School and became a member of the research faculty.

Charles McQueary was appointed by President G. W. Bush as Under Secretary for Science and Technology of the Department of Homeland Security (DHS) and confirmed by the U.S. Senate in March of 2003. Dr. McQueary leads the research and development arm of the Department, utilizing our Nation's scientific and technological resources to provide Federal, State and local officials with the technology and capabilities to protect the homeland.

Prior to joining DHS, Dr. McQueary served as President, General Dynamics Advanced Technology systems, in Greensboro, N.C. Earlier in his career, Dr. McQueary served as President and Vice President of business units for AT&T, Lucent Technologies, and as a Director for AT&T Bell Laboratories.

In addition to his professional experience, Dr. McQueary has served his community in many leadership roles as Chair of the Board, and Campaign Chair, of the United Way of Greensboro; Member of the Board of Trustees of North Carolina Agricultural and Technical State University; Member of the Guilford Technical Community College President's CEO Advisory Committee; Member of Board of World Trade Center North Carolina; Chair for Action Greensboro Public Education Initiative; and as a Member of the Board of Guilford County Education Network.

Dr. McQueary holds both a PhD in Engineering Mechanics and an MS in Mechanical Engineering from the University of Texas, Austin. The University of Texas has named McQueary a Distinguished Engineering Graduate.

Richard Russell was confirmed by the U.S. Senate in August 2002 as Associate Director with the Office of Science and Technology Policy (OSTP) in the Executive Office of the President. As Associate Director he serves as OSTP Director Dr. John Marburger's Deputy for technology. Mr. Russell also serves as Senior Director for Technology and Telecommunications for the National Economic Council. Prior to being chosen by the President for his current position, Russell served as OSTP's Chief of Staff. Mr. Russell also worked on the Presidential Transition Teams for the Department of Commerce, National Science Foundation and OSTP.

From 1995-2001, Mr. Russell worked for the House of Representatives Committee on Science and has a background in technology and environmental policy. The Committee has oversight responsibilities for all Federal civilian research and development and authorizing responsibilities for most civilian science programs.

During his time on the Committee, Mr. Russell helped draft a wide variety of legislation, including efforts to expand and improve coordination of federal information technology research, improve computer security, and authorize agencies such as the National Institute of Standards and Technology. He also was charged with overseeing the committee's technology policy, coordinating its oversight agenda, and helping manage the committee's majority staff.

Mr. Russell began his tenure on the Committee as a professional staff member for the Subcommittee on Energy and Environment. He was promoted to staff director for the Subcommittee on Technology and finally to deputy chief of staff for the full Science Committee. Prior to joining the Science Committee, Mr. Russell was a professional staff member of the Merchant Marine and Fisheries Subcommittee on Oceanography. The Oceanography Subcommittee had jurisdiction over ocean and environmental research and management.

He also directed the Washington office of the Association of California Water Agencies, a nonprofit association representing 400 public water agencies responsible for delivering 90 percent of California's domestic and agricultural water.

Mr. Russell began his career in Washington, D.C. as a research fellow for the Conservation Foundation. He also worked for Congressman Curt Weldon (R-Penn.) and Senator John Seymour (R-Calif.). In 1988 he earned a bachelor's degree in biology from Yale University.

Stratton Sclavos is Chairman and Chief Executive Officer of VeriSign, Inc., a leading provider of intelligent infrastructure services for the Internet and telecommunications networks. Since joining the company in July 1995 as one of its first employees, Mr. Sclavos has helped establish VeriSign as a global corporation relied upon every day by millions of businesses and consumers as they communicate and transact online.

Mr. Sclavos has led the company through a period of robust growth and technology innovation. VeriSign is a billion dollar company with over 2,500 passionate and committed employees worldwide. Over the past few years, he has been honored for his entrepreneurial leadership and management success by numerous organizations including ComputerWorld, Morgan Stanley, Ernst and Young and Forbes magazine. He also sits on the President's NSTAC and is considered an industry expert in cyber security, Internet addressing and converged telecommunications services. He holds a BS in Electrical and Computer Engineering from the University of California, Davis.

Mr. Sclavos also sits on the board of directors of several public and private companies including Juniper Networks and Intuit. A lifelong Bay Area resident and active in the community, Mr. Sclavos and his wife Jody formed the Sclavos Family Foundation to support charitable efforts in children's education and medical research.

Wim Sweldens is the Computing Sciences Research Vice President at Bell Laboratories, Lucent Technologies. He heads the computer science and software research activities in Bell Labs with a focus on security, software quality, systems, applications, and scientific computing. He also manages the relationship between Bell Lab Research and the Lucent Worldwide Services business unit and is responsible for bringing Bell Labs innovations into services.

Dr. Sweldens received his PhD in Computer Science in 1994 from the Katholieke Universiteit Leuven, Belgium, and has been with Bell Labs since 1995. He has conducted research in multi-scale signal processing, computer graphics, and wireless communications. He is the inventor of the lifting scheme, a new wavelet construction and transformation method which has been included in the JPEG2000 standard. The Massachusetts Institute of Technology's 'Technology Review' chose him in 1999 as one of the 100 most promising young innovators. In 2003 he was elected to fellow of the IEEE for contributions to multi-resolution methods for image and 3D geometry compression.

Mike Tiddy is a Senior Manager of Global Government Affairs for Lucent Technologies in Washington, D.C. He has been in his current position since October of 2003. At Lucent, Mr. Tiddy is principally responsible for directing and tracking Lucent's Capitol Hill activities and directing the operations of the Global Government Affairs office. He is also the primary Capitol Hill representative for Bell Labs Innovations.

Mr. Tiddy came to Lucent directly from the United States Marine Corps where he had served as a Communications and Data Systems Officer since 1990. Most recently, he was the Deputy Director of the Marine Corps Senate Liaison Office where he was responsible for developing and communicating the Marine Corps' legislative agenda to the United States Senate. Prior to that Mr. Tiddy was the Satellite Communications Systems Officer for Headquarters, Marine Corps and an Infantry Battalion and Regimental Communications / Data Systems Officer at Camp Pendleton, CA.

Mr. Tiddy received his Bachelor of Business Administration degree in Finance from the University of Oklahoma and he holds a Masters of Science in Information Technology Management from the Naval Postgraduate School.

APPENDIX E: OFFER FOR OPEN SUBMISSION

Offer for Open Submission

A traditional call for papers was not conducted for the 2004 NSTAC RDX Workshop. Instead, participants were given the option to voluntarily submit papers related to the topic of trustworthiness of telecommunications and information systems. 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 F: ACRONYM LIST

Acronym List

3G	3rd Generation
ATIS	Alliance for Telecommunications Industry Solutions
BITS	Banking Industry Technology Secretariat
CEO	Chief Executive Officer
CISR	Center for Information Systems Security Studies and Research
CWIN	Cyber Warning Information Network
DETER	Cyber Defense Technology Experimental Research
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DNS	Domain Name Server
DoS	Denial of Service
DSL	Digital Subscriber Lines
EMP	Electromagnetic Pulse
EMIST	Evaluation Methods for Internet Security Technology
EvDO	Evolutionary Data Only
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FY	Fiscal Year
GETS	Government Emergency Telecommunications Service
GEWIS	Global Early Warning Information System
HSARPA	Homeland Security Advanced Research Projects Agency
HSPD	Homeland Security Presidential Directive
IAIP	Information Analysis and Infrastructure Protection
IP	Internet Protocol
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
ISP	Internet Service Provider
IT	Information Technology

LRTF	Legislative and Regulatory Task Force
MPLS	Multi-Protocol Label Switching
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NGN	Next Generation Network
NGNTF	Next Generation Networks Task Force
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NS/EP	National Security and Emergency Preparedness
NSF	National Science Foundation
NSTAC	National Security Telecommunications Advisory Committee
OMNCS	Office of the Manager, National Communications System
OSTP	Office of Science and Technology Policy
PSTN	Public Switched Telephone Network
QoS	Quality of Service
R&D	Research and Development
RDTF	Research and Development Task Force
RDX	Research and Development Exchange
S&T	Science and Technology
SBGP	Secure Border Gateway Protocol
SCADA	Supervisory Control and Data Acquisition
SMS	Short Message Service
SPF	Sender Policy Framework
SPIM	Spam over Instant Messaging
SPIT	Spam over Internet Telephony
SRAS	Special Routing Access Service
SS7	Signaling System 7
TATF	Trusted Access Task Force
TSP	Telecommunications Service Priority
Wi-Fi	Wireless Fidelity
WiMAX	Wireless Interoperability for Microwave Access
WMD	Weapons of Mass Destruction
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network