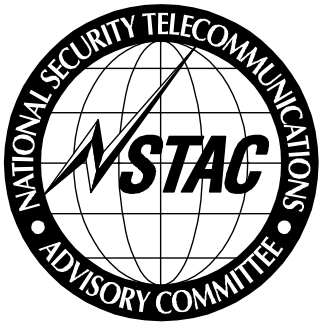

RESEARCH AND DEVELOPMENT EXCHANGE PROCEEDINGS:

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

A SYMPOSIUM SPONSORED BY THE PRESIDENT'S NSTAC IN CONJUNCTION WITH THE WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY AND THE GEORGIA TECH INFORMATION SECURITY CENTER AT THE GEORGIA INSTITUTE OF TECHNOLOGY

GEORGIA INSTITUTE OF TECHNOLOGY
ATLANTA, GEORGIA
MARCH 13-14, 2003

MEMORANDUM FOR THE INDUSTRY EXECUTIVE SUBCOMMITTEE

SUBJECT: 2003 NSTAC Research and Development Exchange Proceedings

On March 13-14, 2003, the President's National Security Telecommunications Advisory Committee (NSTAC) held its fifth Research and Development (R&D) Exchange, in co-sponsorship with the White House Office of Science and Technology Policy (OSTP) and the Georgia Tech Information Security Center (GTISC) at the Georgia Institute of Technology. The event was hosted at the Georgia Centers for Advanced Telecommunications Technology in Atlanta, Georgia. The purpose of the event was to:

1) Explore and prioritize key R&D issues related to the trustworthiness of national security and emergency preparedness (NS/EP) telecommunications and the related, networked information systems;

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

3) Provide input to the OSTP in its preparation of the President's R&D agenda and budgetary requests; and

4) Identify and characterize barriers and impediments that inhibit the R&D of trustworthy networked information systems.

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: a sense of frustration and urgency regarding what they perceived as a lack of substantive action on cyber security issues; the need to improve threat identification and analysis and improve methods to share and use that information across industry, Government, and academia; the need to strike a balance between better engineering of software and hardware with efforts to improve human factors; and the realization that the definition and nature of NS/EP telecommunications continued to change.

The insights, conclusions, and recommendations contained within these Proceedings result from the Exchange and are solely attributable to the combined and unique contributions of Exchange participants and invited speakers. The results indicate that the Industry Executive Subcommittee and the NSTAC should continue to work with OSTP and other NSTAC stakeholders to explore key issues related to R&D of NS/EP telecommunications and information systems.

The R&D Exchange Task Force greatly appreciates the support of the OSTP, Georgia Tech, and our breakout session facilitators. In particular, we thank the Director of OSTP, the Honorable Dr. John H. Marburger, for his personal engagement, which contributed greatly to the event's success. We thank Dr. Seymour E. Goodman, Professor of Computing and International Affairs,

Georgia Tech, and Co-Director, GTISC, for his untiring support and contributions. We are grateful as well to the many staff and contract support contributors who performed so well, attending to so many details. Finally, many thanks to the co-sponsoring companies acknowledged in the Proceedings.

Respectfully,

Guy L. Copeland, CSC
Chair, Research and
Development Exchange 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 fifth Research and Development (R&D) Exchange held in conjunction with the White House Office of Science and Technology Policy (OSTP) and the Georgia Tech Information Security Center at the Georgia Institute of Technology from March 13 to 14, 2003, in Atlanta, Georgia. NSTAC would especially like to acknowledge the important contributions of the OSTP; the Office of the Manager, National Communications System; and the Georgia Institute of Technology for the planning of the 2003 R&D Exchange.

Special thanks also go to our Keynote Speaker, the Honorable Dr. John H. Marburger, Director, OSTP; our Luncheon Speaker, Mr. F. Duane Ackerman, Vice-Chair of the President's NSTAC, and Chairman and Chief Executive Officer, BellSouth; and our hosts at the Georgia Institute of Technology, Dr. G. Wayne Clough, President of the Georgia Institute of Technology; Dr. Richard DeMillo, Imlay Dean of Computing and Director, Georgia Tech Information Security Center; and Dr. Seymour Goodman, Professor of Computing and International Affairs, and Co-Director of the Georgia Tech Information Security Center. We would also like to thank our breakout session facilitators, Dr. Carl Landwehr, National Science Foundation; Mr. Sami Saydjari, Cyber Defense Agency; Mr. David Barron, BellSouth; Dr. Marisa Reddy, U.S. Secret Service; Mr. Michael Vatis, Dartmouth College; Mr. Scott Charney, Microsoft; Dr. Stephen Squires, Hewlett-Packard; Mr. Shannon Kellogg, Information Technology Association of America; Mr. Phillip Lacombe, Veridian; and Mr. Jim Craft, Raytheon.

Finally, NSTAC would like to thank the following organizations for sponsoring the 2003 NSTAC R&D Exchange:

Conference Co-Sponsors

NSTAC Sponsors of R&D Exchange Events

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF FIGURES

EXECUTIVE SUMMARY

From March 13 to 14, 2003, the President's National Security Telecommunications Advisory Committee conducted its fifth Research and Development (R&D) Exchange entitled, *Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness (NS/EP)*. The event was co-sponsored by the White House Office of Science and Technology Policy and the Georgia Tech Information Security Center at the Georgia Institute of Technology. Its purpose 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.

Increasing reliance on the public switched network, the Internet, and computer applications to support national, homeland, and economic security, emergency preparedness, and public safety places a premium on "trusted" systems and networks. The September 11, 2001, terrorist attacks demonstrated the critical importance of networked information systems in supporting national crisis management and response. Ensuring that national leaders, first responders, infrastructure owners and operators, and the general public receive timely, accurate, and complete information through trustworthy NS/EP telecommunications—and the underlying networked information systems—is crucial to meeting national security and homeland security objectives.

To date, a majority of the research studies and activities on the trustworthiness of network 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 threats (e.g., exploitation by insiders, physical destruction) that extend beyond cyberspace. As a result, the sponsors chose to adopt a broad perspective for the R&D Exchange, exploring 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;
- **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;
- **Physical Security –** protecting physical assets (e.g., facilities, equipment) from damage, destruction, and exploitation; and
- **Integration –** managing and integrating innovative R&D to build trusted tools and systems to support future NS/EP telecommunications infrastructures and applications.

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

- **A strong sense of frustration and urgency.** Participants noted the R&D Exchange was but one of many conferences and events focused on issues of trustworthiness and

security. They commented that each event produced similar results and recommendations, but that action and implementation were fleeting. At the same time, however, they conveyed a strong sense of urgency about trustworthiness topics. Participants agreed that, given the global nature and increasing proliferation of distributed denial of service attacks and computer viruses, grappling with how to prevent and mount effective responses to such types of attacks was a pressing national issue requiring senior-level attention and commitment in industry, Government, and academia.

- **A need to clarify the definition of NS/EP telecommunications in the post 9/11 world.** An issue frequently discussed at the event was the changing nature of NS/EP telecommunications. Participants noted the changing threat environment (from Cold War to distributed threats posed by rogue states and international terrorist groups), evolving technologies (from the traditional public switched network to a converged network composed of traditional voice services, wireless services, the Internet, etc.), and creation of new Government institutions (the Department of Homeland Security) all generated a need to clarify the meaning of NS/EP telecommunications in the post-September 11th environment. They also agreed that a better understanding of NS/EP telecommunications might serve as a catalyst for, and offer a rationale for, prioritizing R&D in key security technology areas.

- **A need to address major challenges on driving technology innovation into NS/EP systems and functions.** The complexity associated with driving technology innovation into NS/EP systems and functions derives from the lack of an overall system architecture that incorporates trust in each system layer, starting from devices, components, systems software, and working through all the applications layers. Research needs to be vertically integrated across these layers and mechanisms developed to identify and integrate technologies related to trust. Consensus on the unprecedented needs and capabilities indicates a need for rapid prototyping and testbeds to assure the desired integration into future NS/EP systems.

- **A need to establish partnerships for R&D integration.** Government funding is a critical component to success in trustworthiness, but it is not the overriding factor. The most important factor is adopting an R&D strategy that will attract participation from all the technology, industry, and user sectors to drive the integration into the real systems. The challenge is to attract the operations elements of industry to provide resources and assets, including people, access to real systems, and funding to conduct tests in collaborative and innovative research projects, pilots, and testbeds. Economic incentives need to be created for all sectors to cooperate and interoperate on R&D.

- **A need to influence business drivers for security.** Historically, public research was the primary driver for technology innovation and development in the United States. During the Cold War, the research community relied in the main on U.S. Government funding and direction. In the 1990s, however, this model evolved with private funding of research and technology development equaling and exceeding Government investment. Recognizing the shortage of available resources (Government R&D funds and grants, capital investment in industry, budget cutbacks at universities), participants discussed the need to collaborate on ways to stimulate and leverage market forces as a catalyst for developing the next generation of security tools and products.

- **A need to improve threat definition and analysis and, equally important, identify methods to share and analyze that information to influence R&D.** Participants agreed that understanding the evolving capabilities and intent of potential adversaries (nation-states, terrorists, hackers, insiders) was an important element in developing security tools and products that would meet the future needs of industry, Government, and academia. Participants noted that it was crucial to future R&D to develop a baseline of existing telecommunications and computer networks and to invest in enhancements to the Internet that would allow for regular and more real-time monitoring of Internet health, modeling, simulation, analysis, and testing of new vulnerabilities.

- **A need to strike a better balance between better engineering of software and hardware with efforts to improve human factors.** Participants noted the importance of having a well-trained and educated workforce, consistent and enforced policies, and a better understanding of the motivations and actions of insiders. A concern regularly expressed at the event was that every action taken in one realm (cyber, human factors, physical, integration) had both visible and often hidden impacts on the other.

RESEARCH AND DEVELOPMENT EXCHANGE

PROCEEDINGS

1. 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 March 13 to 14, 2003, the President's NSTAC conducted its fifth Research and Development (R&D) Exchange entitled, *Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness*. The event was co-sponsored by the White House Office of Science and Technology Policy (OSTP) and the Georgia Tech Information Security Center at the Georgia Institute of Technology. Its purpose was to stimulate an exchange of ideas among researchers and practitioners from the telecommunications industry, Government, and academia on issues regarding trustworthiness.

1.1 BACKGROUND

Increasing reliance on the public switched network, the Internet, and computer applications to support national, homeland, and economic security, emergency preparedness, and public safety places a premium on "trusted" systems and networks. The September 11, 2001, terrorist attacks demonstrated the critical importance of networked information systems in supporting national crisis management and response. Ensuring that national leaders, first responders, infrastructure owners and operators, and the general public receive timely, accurate, and complete information through trustworthy NS/EP telecommunications—and underlying networked information systems—is crucial to meeting national security and homeland security objectives.

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." 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 and studies focused on trustworthiness have concentrated on vulnerabilities in cyberspace. However, achieving and sustaining trustworthiness in those systems is jeopardized by a host of threats (e.g., physical destruction, exploitation by insiders) that extend beyond cyberspace. As a result, the sponsors of the R&D Exchange chose to adopt a broad perspective, exploring the full range of trustworthiness issues as they pertained to NS/EP telecommunications and information systems. Specifically, the exchanged 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, and an inconsistency in patch implementation.

- **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.

- **Physical Security –** as the September 11, 2001, attacks clearly demonstrated, trusted systems could be compromised via damage to and/or infiltration of the physical locality in which the system was housed. Damage to the facility itself may be caused by a variety of environmental and man-made factors (e.g., hurricanes, earthquakes, cable cuts, terrorist attacks) and has the potential to destroy, disable, or corrupt trusted systems. In addition, vulnerabilities in site protection (e.g., lack of security guards, access controls) leave trusted systems susceptible to tampering from internal and external threats.

- **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. As technology continues to evolve and vendors produce new proprietary solutions, network providers and users face new challenges in integrating new applications and products with legacy systems to produce secure and trusted systems across an entire enterprise.

1.2 PURPOSE

The purpose of the R&D Exchange was to facilitate a dialogue among industry, Government, and academia to discuss the cyber security and software, human factors, physical security, and integration issues associated with the trustworthiness of NS/EP telecommunications and information systems. To stimulate robust discussion, facilitators and participants were selected to present the views of the vendor, network provider, academic, and Government communities.

1.3 PROCEEDINGS ORGANIZATION

This Proceedings document provides an overview of the 2003 R&D Exchange. Specifically, it is divided into six sections and associated appendices:

- Section 1 presents background information on the 2003 R&D Exchange;

- Section 2 reviews the opening plenary session and the keynote address by the Honorable Dr. John H. Marburger, Director of OSTP;

- Section 3 summarizes the luncheon address from Mr. F. Duane Ackerman, Vice Chair of the President's NSTAC and Chairman and Chief Executive Officer, Bell South;

- Section 4 captures the observations and findings from the Exchange's breakout sessions;
- Section 5 highlights discussions from the closing plenary session;
- Section 6 presents the major findings from the 2003 R&D Exchange; and
- Appendices include the agenda, attendees, speaker remarks, speaker and facilitator biographies, and other conference materials.

2. OPENING PLENARY SESSION

The opening plenary session to the 2003 R&D Exchange commenced with opening remarks from Dr. Seymour Goodman, Professor of Computing and International Affairs and Co-Director of the Georgia Tech Information Security Center and from Dr. G. Wayne Clough, President of the Georgia Institute of Technology. Dr. Goodman welcomed participants to the 2003 R&D Exchange, and Dr. Clough introduced the Honorable Dr. John H. Marburger, Director of the White House Office of Science and Technology Policy (OSTP).

2.1 KEYNOTE ADDRESS

Dr. Marburger opened his remarks by thanking the exchange sponsors and stating his office was counting on the results from the R&D Exchange to serve as input to guidance OSTP would provide the Office of Management and Budget and other White House offices on funding R&D objectives and priorities. He emphasized that advice from experts and practitioners in industry, Government, and academia remained vitally important to helping promote a cultural change in how people use technology and consider security in their day-to-day lives.

Dr. Marburger then described the changing operating environment influencing NS/EP telecommunications. He reviewed the Administration's decision to create a Department of Homeland Security (DHS), noting it represented the single largest Government reorganization in a half-century. In addition, on February 28, 2003, President George W. Bush signed an omnibus of Executive Orders (E.O) related to the transfer of many Government functions and activities to the new Department. He explained that two E.O.s, 12472 and 12382, and a new Homeland Security Directive (HSD) 5, were of particular relevance to the NS/EP telecommunications mission and the President's NSTAC.

Dr. Marburger then stated the Nation must continue to leverage its extensive R&D resources in support of enhanced NS/EP telecommunications capabilities that would ensure an effective and timely response to crises. He referenced the numerous organizations and advisory committees composed of representatives from industry, Government, and academia that supported OSTP efforts, but emphasized the importance of specifically soliciting the expertise of the President's NSTAC. In particular, Dr. Marburger stated that as the owners and operators of the Nation's telecommunications and information infrastructure, NSTAC advice and council was crucial during all phases of R&D, from basic research through development and fielding. Concluding his remarks, Dr. Marburger acknowledged the complications caused by the growing Federal budget deficit and financial difficulties in industry, noting the limits those imposed on new R&D funding. However, he stated that despite such limitations, the Administration's proposed fiscal year (FY) 2004 budget submission included $123B in new funding targeted to homeland security and defense, representing a 7 percent increase over FY 2003.

In the question and answer period, a participant asked about international cooperation with respect to R&D. Dr. Marburger replied that during his last visit to Europe, many science ministers expressed a strong interest in collaborating on scientific and technological research initiatives, particularly in the cyber arena. He noted that potential conflicts, such as competition exist, but that the United States needed to continue efforts to reach out to other countries to advance security research. Dr. Marburger also suggested that international standards bodies could prove a useful bridge between companies and countries in researching, developing, and fielding new technologies.

Another participant inquired about the Administration's priorities with respect to critical infrastructure protection. Dr. Marburger stated that the September 11, 2001, attacks clearly illustrated some of the Nation's vulnerabilities to attack, specifically buildings, transportation assets, and telecommunications. Of specific relevance to the Exchange, Dr. Marburger said the President believed information technology (IT) was an essential enabler in securing the homeland, and the Administration was exploring strategies to maximize R&D funding and investments. In response to a related question about Federal funding and coordination of R&D focused on homeland security issues, Dr. Marburger stated that a linchpin of the President's *National Homeland Security Strategy* was to harness technology to protect the homeland, and that the Homeland Security Act had created the Science and Technology Directorate within the new Department to serve as the focal point for R&D.

(Note: the full text of Dr. Marburger's presentation is attached in Appendix C)

2.2 NSTAC OVERVIEW

Following the keynote address, Mr. Guy Copeland, CSC and R&D Exchange Chair, briefly reviewed the core missions, functions, and membership of the NSTAC for those unfamiliar with the organization. He noted the NSTAC had conducted R&D Exchanges with representatives from industry, Government, and academia since 1991 on a variety of important R&D topics related to NS/EP telecommunications activities.

Mr. Copeland then 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 I	Scott Charney, Microsoft Phillip Lacombe, Veridian
Cyber Security and Software II	Carl Landwehr, National Science Foundation Sami Saydjari, Cyber Defense Agency
Human Factors	Marisa Reddy, U.S. Secret Service Michael Vatis, Institute for Security Technology Studies at Dartmouth College
Physical Security	David Barron, BellSouth Jim Craft, Raytheon
Integration	Stephen Squires, Hewlett-Packard Shannon Kellogg, Information Technology Association of America

3. LUNCHEON PRESENTATION

Mr. F. Duane Ackerman, Vice Chair of the President's NSTAC and Chairman and Chief Executive Officer, BellSouth, opened his remarks by emphasizing the importance of keeping research and technological innovation at the forefront of national priorities. He said that need was particularly true in the area of telecommunications and information technology, which acted as the Nation's "central nervous system." With that in mind, he highlighted two tensions associated with advances in telecommunications and information technologies. First, Mr. Ackerman described how the unprecedented connectivity offered by the telecommunications industry and the Internet was at once both a source of national strength and vulnerability. He said that advancing technology had afforded citizens greater access to a rich set of voice and data services, but also had introduced new risks to the public switched network. Specifically, he cited the recent "SLAMMER" worm, which became the fastest spreading computer virus ever recorded. Second, Mr. Ackerman noted a growing disconnect between the pace of technology development and the ability to manage that technology. Specifically, he emphasized the rapid introduction of new technologies was outstripping finely tuned corporate policies and processes designed to manage networks.

Mr. Ackerman underscored how industry depended on both public and private science to fuel technology evolution and integration. Specifically, he identified three areas requiring the attention of both the research community and national policy makers. The first was the need to harden telecommunications networks. With more than a billion access points on the Internet, he emphasized the need to promote research in the areas of network management interfaces and configuration control and management. The second area was the need for better tools and technologies to detect attacks against and defend telecommunications networks. Specific research areas requiring attention included network wide pattern recognition, anomaly detection, and new detection tools analyzing packet flows. Third, Mr. Ackerman commented on the need to research technologies that would enable networks to adapt to and survive attacks. Examples include technologies to manage traffic and to compartmentalize or isolate network damage.

Transitioning his focus to the importance of national policy and partnership, Mr. Ackerman pointed to the importance of economic security as a component of homeland security. He also recognized the importance of technology in addressing the Nation's homeland security risks and described how economic and investor uncertainties have created an investment gap in research and development. Mr. Ackerman reflected on how America had always prospered from innovation and the development of new technologies. He stated that a national priority should be to stimulate and unleash a new wave of investment in science and technology. Concluding his remarks, Mr. Ackerman noted the importance of trust and a "network of partners" to secure telecommunications networks and the Internet. Specifically, he pointed to the need to identify a common ground among those partners in the areas of standards, priorities, and best practices that would serve as the foundation for trustworthiness.

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

4. BREAKOUT SESSIONS

To facilitate discussion of trustworthiness issues, participants divided into five breakout sessions (two cyber security and software groups, human factors, physical security, and integration) and were asked to consider the following questions:

- What is the current state of affairs with respect to R&D of your issue? What technologies, or other research avenues, offer the most promise?
- What technology areas offer the most potential to improve the security of trusted systems? Which area(s) warrant the most attention?
- What impediments might inhibit further R&D?
- 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 are the underlying policy issues that should be studied by the President's NSTAC or other body?
- What would be your three to four key points related to developing an agenda for action on trusted NS/EP telecommunications?

Observations and results from the breakout sessions are presented as follows.

4.1 CYBER SECURITY AND SOFTWARE, GROUP I

The Cyber Security and Software Group I began its discussions by emphasizing how the digital revolution had permanently altered the way our society functioned. Participants noted that almost every aspect of daily life depended in some manner on the telecommunications and information infrastructure. They stated the delivery of Government services, the conduct of business transactions, and the assurance of national security and public safety missions all relied on information technologies and systems. Participants agreed those systems had dramatically increased productivity and commercial efficiency, but also had exposed users to new security breaches, cyber attacks, and unpredictable, cascading effects. Many acknowledged that developing trustworthy computer systems should be considered a major research priority and be funded accordingly.

4.1.1 The Current Operating Environment

Participants determined that protecting NS/EP mission-critical systems and ensuring their reliability had become a responsibility not only of the U.S. Government but also that of the private sector, the primary owner and operator of critical infrastructure. Participants emphasized that the Nation needed to expect and, in turn, develop strategies to eliminate more sophisticated threats likely to be unleashed in the future. They noted today's security practitioners were responding to hackers defacing web sites or stealing credit card numbers. In the future, however, highly organized terrorist organizations (and possibly hostile foreign countries) might launch more sophisticated, widespread, and debilitating attacks, exploiting vulnerabilities in the information infrastructure.

Several participants noted how R&D investments in cyber security were minimal in the 1980s, and how the results of that neglect were visible today. They stated the increasing reliance on

commercial off-the-shelf (COTS) products had reduced overall cost, but also caused users to become dependent on third party vendors for the design and security of important components. Others stated the U.S. Government, reluctant to regulate the Internet to avoid stifling competition, had mainly delegated the responsibility to protect the Nation's critical telecommunications infrastructure to the private sector. They noted, however, that market objectives and national security concerns were not always harmonious. They stated the primary motivation for a company was to increase profitability and market presence. Therefore, most participants agreed that reliance on pure market forces was unlikely to produce a business case conducive to spending valuable resources on security protections. The group also expressed an overall sense of frustration at the political and bureaucratic processes driving research in cyber security technologies, noting many of today's security vulnerabilities were identified more than a decade ago, but little progress had been made in eliminating them.

4.1.2 Research Priorities

For the United States to maintain its technical edge in cyber systems, the Cyber Security and Software Group I participants recommended that OSTP should focus on R&D activities in two dimensions: (1) *short-term research* that could improve the trustworthiness of software and cyber systems in the near future and (2) *long-term research* that could embed the concept of trustworthy computing in the design of future systems (all priorities are summarized in Figure 1).

Figure 1. Cyber Security and Software, Group 1 Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Economic Incentives	• Develop and encourage the creation of market incentives designed to stimulate research in security technologies. Those incentives could include, but not be limited to, tax breaks and credits, subsidies, or any other monetary incentives
Vulnerabilities	• Develop methods and tools to eliminate vulnerabilities in software during the design and development phases, particularly with source code • Develop techniques to automatically test for vulnerabilities in COTS • Develop validation and quality assurance techniques to ensure that appropriate software patches are installed • Develop and deploy computer security embedded measures (e.g. trustworthy code, secure default mechanisms)† • Design compilers to scan source code and identify, if not remove, vulnerabilities†
Secure Protocol Design and Development	• Promote secure protocol design by analyzing current routing and signaling protocols (e.g. BGP) and incorporating findings into the design of future protocols
Legacy System Security	• Implement techniques to strengthen the security of legacy systems
Priority Routing	• Develop a GETS-like program for priority packet routing in all networks with assured quality of service for use during emergency situations
Modeling and Simulation Mechanisms	• Develop modeling, simulation, and analytic techniques and mechanisms to pinpoint systemic weaknesses and better prepare for and respond to emergencies • Model and simulate networks to map network topologies and monitor Internet traffic • Develop early warning systems to prevent and respond to cyber attacks†
System Wide Recovery and Remediation	• Improve system wide recovery and remediation to create more robust network systems that respond more quickly to attacks
Intelligent Agents	• Research methods, such as intelligent agents, to monitor traffic electronically, configure systems, and enforce security policies automatically
Information Sharing	• Determine what information should be shared among infrastructure owners • Create data collection system to help generate a business model for sharing

RESEARCH AREA	RECOMMENDED FOCUS
Risk Assessments	• Promote the development of risk assessment methodologies to help analyze the costs associated with implementing/not implementing security mechanisms
Best Practices	• Conduct impact analyses to assess the efficacy of best practices and evaluate how they are implemented
Cyber Security Research	• Support basic research in the science of cyber security to include building and deploying inherently secure architectures; testing and evaluating large-scale systems; defining rules of composition for large-scale systems; and defining and developing technical metrics that measure the strength of security† • Design compilers that eliminate or (at least) identify vulnerabilities during compilation of software applications
Embedded Systems	• Promote the security of "embedded systems" where old architectures have been integrated into new, more security-oriented architectures†
Advanced Investigative Tool Development	• Develop tools for authentication, forensics, and attribution to facilitate international investigations and foster cooperation†

† Denotes Long-Term Focus

4.1.3 The Path Forward

The group concluded the session by discussing several cyber vulnerabilities that must be addressed to improve trustworthiness in the future. Vulnerabilities included Internet Signaling Gateway effects on the traditional public switched network, signaling and routing protocols, peer-to-peer technology, trustworthiness of code, and wireless technology. Participants emphasized that R&D efforts would have to adapt to evolving threats and technologies to be effective. They also noted that solutions identified through the process would have to be implemented at a reasonable cost and in a timely manner.

4.2 CYBER SECURITY AND SOFTWARE, GROUP II

The Cyber Security and Software Group II, began its discussions by scoping the issue of cyber trustworthiness and determining the topics that should be considered and the research that should be developed to support trustworthiness.

4.2.1 The Current Operating Environment

Participants noted the operating environment, and in particular, threats and vulnerabilities surrounding the cyber systems could be characterized in the following manner. They stated that NS/EP networks had operated reasonably in situations of naturally induced faults, errors and failures, and physical attacks. However, they noted that business and economic factors might trigger changes in the trustworthiness of the underlying telecommunications and computing fabric of NS/EP systems. In other words, business decisions to add a new technology or system could directly (or indirectly) affect the trustworthiness of NS/EP telecommunications. They indicated that NS/EP managers charged with acquiring and managing network resources often faced difficult choices among alternatives and lacked a strong rational basis for making decisions affecting system trustworthiness. Complicating matters, responses to reports of new vulnerabilities in NS/EP networks were dealt with largely through intensive manual response. Consequently, the result was NS/EP networks and components that are significantly vulnerable to malicious attacks that exploit naturally occurring faults and errors and that could be significantly more vulnerable to sophisticated attacks.

4.2.2 Research Priorities

After characterizing the current environment, participants then identified critical research needs that should be fulfilled to build systems with trusted cyber and/or software components (see Figure 2).

Figure 2. Cyber Security and Software, Group II Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
System Criticality	• Determine the criticality of specific systems to better understand the potential impact of specific system vulnerabilities and to rationalize and prioritize investments to protect, mitigate, and eliminate those with the greatest potential economic/performance impact
Security Metrics	• Develop and verify security metrics for use on a national level to create a much-improved environment and common format for sharing intrusion information
Information Assurance Decisionmaking	• Develop decision support tools to help organizations better understand how security products and applications might impact system performance and assess economic impacts (e.g., return on investment)
Internet System Dynamics	• Develop a clearer understanding of the Internet's system dynamics including reconciling the security roles, responsibilities, and relationships between the "end-nodes" and the intermediaries • Create a national cyber command and control system to develop and implement a national process for cyberspace indications and warning and develop national benchmarks for trustworthiness of NS/EP telecommunications systems based on different levels of criticality that would improve the health of the Internet
Well-Trained Workforce	• Promote the development of a more well-trained workforce for research, development, and operation • Increase emphasis on security, trustworthiness, and cyber ethics at academic and training institutions
Trustworthiness	• Improve the "building blocks" of trustworthiness – better attribution and damage prevention/limitation
Policy Development	• Develop policy fostering cooperation, collaboration, and prosecution for the mutual protection of national and international infrastructures

4.2.3 Impediments to R&D

The Cyber Security and Software Group II participants identified six impediments to building trusted NS/EP telecommunications and information systems. First, they stated there was a shortage of trained operators and researchers dedicated to the concept of trustworthiness. Without trained personnel, adequate advances in trusted networking technology would not be developed, deployed, and utilized universally. Second, participants noted that short of a widespread disaster, many organizations did not see the value in dedicating the necessary funds to R&D activities targeted to establishing trustworthiness. Third, no clearinghouse existed to facilitate the sharing of information on relevant R&D programs. Participants suggested that the establishment of such a clearinghouse would allow for easier access to important data and the ability for groups undertaking the same research to more effectively share information and collaborate. Fourth, participants noted the detrimental effect of outsourcing software/hardware manufacturing, especially to offshore locations. Fifth, some participants noted the difficulty in quantifying the benefits of new security products resulting from R&D programs. Finally, participants said there were not uniform critical infrastructure protection standards for minimum security for use in the procurement process. They stated that without such standards, networks would continue to be secured unevenly.

4.2.4 The Path Forward

The group developed three main recommendations for future action:

- **Set a national vision for trustworthiness of NS/EP telecommunications –** to do so, participants asserted the concept of trustworthiness must be clearly defined in order for industry, Government, and academia to work together successfully. Participants agreed the definition should include levels of trustworthiness so that one system could be declared more or less trustworthy than another system.

- **Develop scientifically validated and compelling "national security" cases for the vulnerability of existing NS/EP telecommunications systems –** participants noted that such a recommendation was important because many decisionmakers in industry and Government neglected to place enough emphasis on the importance of trustworthy systems. If a convincing national security case could be presented to senior Government officials, the flow of additional Federal funds might help create a market that stimulated additional private investments.

- **Work with key White House agencies to secure the necessary funding to realize the vision –** participants agreed that combining the national vision with a compelling national security case for investment was important, but equally vital was working closely with key White House agencies (e.g., OSTP, Office of Management and Budget) to ensure that R&D priorities in the security arena were incorporated into the President's annual budget submission.

4.3 HUMAN FACTORS

Participants emphasized the fact that human factors pervade all aspects of trustworthiness in NS/EP telecommunications and information systems. In particular, participants noted the human element was a vital component when considering efforts to develop, maintain, and sustain trustworthiness in NS/EP telecommunications and information systems. The efficacy of any technology directly depends on the ability of humans to design, develop, configure, implement, and manage it. Even the best technical solution can prove vulnerable to intentional (e.g., external attack, insider threat) or unintentional acts (e.g., defective software, inadequate system configuration, non compliance with security policies).

4.3.1 The Current Operating Environment

The Human Factors session participants identified seven broad areas shaping the operating environment focused on 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.

- **Policy Development, Dissemination, and Enforcement –** participants cited the lack of 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 disseminated to all staff, and their implementation was enforced, remained important aspects of maintaining trustworthiness.

- **Human Processing and Decision-Making –** participants highlighted how assisting humans to process information about, and make decisions on, security matters was a crucial element in ensuring trustworthiness. Concerns were expressed both about instances where humans were required to process too much information in making a decision and other situations where not enough information was available to decision-makers. The need for R&D on ways to enhance decisionmaking about security during conditions of uncertainty was emphasized.

- **Anomaly Detection –** participants noted that while there was considerable research in the computer security field on anomaly detection, there was a need to examine R&D efforts in other disciplines (e.g., weather forecasting, sonar) that also might apply to securing NS/EP telecommunications and information systems. Participants recommended that applying anomaly detection research from computer security and other disciplines to address both cyber and physical issues was important to building trusted systems.

- **Insider Threats –** participants discussed the need to both examine those who violated a trust relationship and situations where employees were deterred or received incentives for not violating that trust. Participants recommended devoting additional research to understanding the psychology of what motivated insiders in exploiting system vulnerabilities.

- **Cultural Shifts –** participants highlighted the need to influence a cultural shift that would encourage users and managers alike to embrace security, both from the top-down and bottom-up. Specifically, participants emphasized the importance of establishing strong governance processes (e.g., accountability, enforcement) that emanated from senior management coupled with training and awareness programs that would heighten the sensitivity of employees to security concerns.

- **Source of Supply –** participants noted the importance of being able to determine whether a software application or hardware 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 hardware that could be exploited at a later date. Participants also discussed the need to develop a process to assess the threat posed by specific software and hardware suppliers.

4.3.2 Research Priorities

The Human Factors session participants identified five key areas for research (see Figure 3).

Figure 3. Human Factors Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Human Processing and Decisionmaking	• Leverage knowledge accrued from other risk management disciplines (e.g., banking, transportation, public health) to minimize biases and risks related to information security • Enhance tools and technologies to improve human decisionmaking under conditions of ambiguity or uncertainty • Reduce impact of human factors (e.g., number of humans interfacing with key systems) by making security transparent
Anomaly Detection	• Research automated tools/techniques to detect anomalies (both physical access and cyber) across an entire enterprise • Research tools to better visualize/interpret outputs in real or near real-time from highly complex detection/anomalous activity systems (e.g., replace audit logs)
Education, Training, and Awareness	• Educate, train, and increase awareness of security issues (e.g., conduct market research on effective techniques to raise awareness across demographic divides)
Insider Threats	• Investigate true prevalence of insider incidents (e.g., frequency, impact) • Research cultural, psychological, technical, and organizational factors that both motivate and deter insiders (e.g., what motivates an insider to act; what prevents others from exploiting known vulnerabilities) • Research tools and techniques to better combat insider threats • Translate insider threat research (existing/ongoing) into useful techniques and policies
Supply Source	• Explore multiple, distributed venues for checking source code (e.g., coordination with IA Centers of Excellence) • Validate distribution processes • Prioritize what code needs to be checked

4.3.3 Impediments to R&D

The Human Factors session identified three overarching impediments to building trusted NS/EP telecommunications and information systems. First, they agreed that a balanced approach to security was often lacking. Specifically, they stated good security resulted from a combination of consistent and enforced policies and procedures, robust technology, and well-educated users and managers. Participants said that in today's environment, many viewed those three factors as a zero-sum game, i.e., high-end technical solutions offered better "fixes" to security vulnerabilities, but might be difficult to use and too technically complex for the average system user. Second, participants described the need to articulate and quantify the value of security. One participant commented, "no matter the sophistication of the technology or its simplicity of use, they create an additional burden [in the form of investment or maintenance costs]." A common problem cited during the session was that security was difficult to quantify because the costs were concentrated (e.g., applications, equipment, personnel), but the benefits were distributed across an entire enterprise and not easy to quantify in terms of a return on investment. Third, a host of legal, jurisdictional, definitional, and cultural issues emerged as significant impediments. Specifically, discussions focused on the need to: (1) improve information sharing among industry, Government, and academia; (2) stimulate higher reporting on crimes (e.g., cyber

attacks, insider incidents); and (3) explore the meaning and definition of NS/EP in light of the post-September 11, 2001, environment.

4.3.4 The Path Forward

A major theme in the Human Factors session was a general sense of the need to generate breakthrough ideas. Participants noted that many of the issues discussed in the session were not new. Suggestions to improve training and awareness programs or examine the insider threat were well-documented recommendations from other conferences and seminars on trusted computing and cyber security. That said, the participants identified key areas where they believed new research could bear fruit:

- **Explore paradigm-shifting research in other sectors (e.g., healthcare, weather forecasting) that might offer new insights into information security –** participants noted that in the area of anomaly detection, for example, research extended beyond computer security into the fields of weather forecasting, sonar systems, geological surveys, and mineralogy—might a breakthrough in one of those disciplines translate to the information security field?

- **Research usable, cost effective, and interoperable multi layer technologies for authentication and authorization –** participants cited biometrics as an example of a promising technology that required continuing research and applied development to make it a more affordable solution for access control.

- **Research ways to identify suppliers whose products might pose a threat to NS/EP telecommunications and information systems –** participants determined that given the growing dependency of the U.S. Government on COTS technology (both produced domestically and abroad), it was important to track where specific software applications (or related source code) and hardware was produced and by whom, and to find ways to assess the threat these suppliers might pose.

- **Study 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.

- **Research offensive tactics and strategies for information security –** participants discussed the need to examine how employing offensive tactics and strategies might deter both insider threats and external attacks.

4.4 PHYSICAL SECURITY

Participants discussed a variety of issues related to taking active measures to mitigate physical security challenges to ensure trustworthy NS/EP telecommunications. Specifically, they outlined the current environment; brainstormed and prioritized research activities that would reduce the possibility of harm done by physical attacks; developed a list of technologies that could be utilized for physical security; and identified major impediments to addressing the broad range of threats and vulnerabilities related to physical security.

4.4.1 The Current Operating Environment

Participants began by characterizing the current state of physical trustworthiness. They agreed on the importance of several overarching themes. First, they stated there was a lack of defined or Government-validated threat scenarios or adversary attack plans against which to build measures for protecting facilities. Second, they noted the difficulty for telecommunications companies to first determine what threats existed to the industry and then protect against all feasible attack techniques. Participants also noted a lack of widespread understanding and appreciation within the industry for the sophistication of threats they face on a day-to-day basis. Finally, participants emphasized physical security must also be thought of in the context of protecting human capital in addition to the more obvious and visible threats to physical assets. In considering R&D issues related to physical security, participants identified the following issues:

- **Physical Access Control –** participants noted that physical access control was a fundamental component in physically protecting a telecommunications asset from unintended and malicious harm. Access control issues included identifying, authenticating, authorizing, and tracking individuals to protect against unauthorized access from outsiders and to limit access by internal users to appropriate personnel. Participants suggested current physical access control may be challenged by insufficient funds to pay for the ultimate in security and social engineering tactics.

- **Information Control –** participants agreed that maintaining control of information regarding the location of cable landings, rights of way, markings, etc., was essential to protecting telecommunications assets. Participants also raised the question of how a telecommunications company should balance protecting its cables from attack while also ensuring that backhoe operators did not mistakenly cut cables while working.

- **Architectural Integrity –** participants noted that with the September 11, 2001, attacks, issues surrounding architectural integrity had gained renewed importance. They noted that telecommunications companies must discuss and develop new ways to protect physical structures against natural and man-made attack techniques. Suggested ideas included revising building codes to include new "immune" building materials and technologies.

- **Education and Awareness –** participants agreed that education and awareness programs were critical to disseminating information on key problems/concerns related to the physical protection of telecommunications assets. They said efforts should be made to warn telecommunications personnel of the threat of social engineering and the need to support basic physical security processes.

4.4.2 Research Priorities

As a result of the discussion, participants developed a prioritized list of research priorities they believe should be further examined through industry/Government/academic partnerships (see Figure 4).

Figure 4. Physical Security Research Priorities

RESEARCH AREA	RECOMMENDED FOCUS
Modeling and Simulation	• Undertake advanced modeling and simulation activities for NS/EP events that include virtual attack/defense of facilities/networks • Develop a "SimFacility" simulation tool (based on SimCity-like capabilities) to better understand vulnerabilities and potential threats to physical infrastructures housing critical network components
Vulnerability Analysis	• Develop better vulnerability analysis to understand critical single points of failure and interdependencies
Biometrics	• Develop industry standards for and implement a biometrics based national standard industrial identification card • Utilize biometric technologies (e.g., iris scanning, hand geometry, facial recognition) to enhance access control processes
Critical Infrastructure Standards	• Investigate standards for the diversity of critical infrastructures
Automated Defenses	• Develop a system(s) for automatic defense of cable routes from backhoes, etc.
Background Checks	• Provide better background checks for people with access to critical facilities
Anomaly Detection	• Develop a process to analyze patterns of facility use (e.g., social engineering, data mining)
Information Availability	• Research the possibility of withdrawing critical vulnerability information from the public domain
Immune Buildings	• Research and develop "immune" building technologies to better secure facilities against biohazard attacks

4.4.3 Impediments to R&D

While participants recognized that many steps could be taken to increase the physical trustworthiness of NS/EP telecommunications systems, they also noted several impediments. First, participants discussed how the Federal Government depended significantly on private industry for the provision of telecommunications services supporting NS/EP activities and how the telecommunications industry itself was a highly competitive, capital intense business. To maintain market share, enhance network architecture(s), preserve customer satisfaction, and deliver stockholder dividends, telecommunications companies must prioritize funding allocations to maximize profits and network growth. Consequently, participants suggested that neither the Federal Government nor telecommunications companies had the financial and/or human resources necessary to protect all physical assets against all modes of attack. They noted that network operators must rely on cost-benefit analyses when determining how best to protect network components. In addition, participants suggested regulatory and other pressures (e.g., Federal tariffs) might limit the security-related investments companies may make.

Second, participants noted that the continually evolving process of identifying and mitigating physical threats and vulnerabilities relies heavily on constructive and effective information sharing between all stakeholders. However, the question remained, "How do you make information available to all relevant parties without increasing the potential for negative exploitation of existing vulnerabilities?" Furthermore, participants noted that the trustworthiness of NS/EP telecommunications depends specifically on trusted information sharing between industry and Government representatives. They said that while established information sharing mechanisms between the telecommunications industry and Government had been incredibly effectual, certain concerns still existed. Participants noted, for instance, how industry and

Government did not always demonstrate mutual trust. In addition, they suggested that industry believed that Government tended to request, but did not always explain the need for, or projected use of, sensitive industry data. Such impediments must be recognized and addressed to ensure paramount physical security of NS/EP telecommunications.

4.4.4 The Path Forward

Physical breakout session participants identified three areas of future research necessary to improve physical security. These areas are:

- Define levels of "critical" and determine what telecommunications assets can be considered critical for NS/EP purposes and interdependencies;
- Determine what threats exist with regard to the telecommunications industry and develop a rapid method for disseminating this information to those in industry who need it; and
- Develop modeling and simulations technology related to protection of those assets deemed critical.

4.5 INTEGRATION

The Integration Group was tasked to examine the macro issues associated with identifying strategies to promote effective integration of R&D innovations. Participants discussed specific mechanisms and strategies to accelerate the transition and integration of innovative R&D to build trusted tools and systems to support future NS/EP telecommunications infrastructures and applications. Consensus on the unprecedented needs and capabilities indicated a need for rapid prototyping and testbeds to accelerate integration into future NS/EP systems.

4.5.1 Current Research and Operating Environments

Participants noted that current NS/EP initiatives, including the Government Emergency Telecommunications Service (GETS) program, operated over the existing telecommunications infrastructure and used current analog and digital telephone services. Participants discussed the need for an updated version for NS/EP systems that would sustain changing technologies. Participants noted that new systems would include a full range of IT functionality and internetworking to enable dynamic collaboration among a wide range of end users and their systems. They suggested that R&D on NS/EP telecommunications systems also needed to interoperate across wireline, wireless, satellite, and future innovations.

In particular, participants noted that NS/EP systems needed to integrate several new functions and capabilities, including fully digital systems. Participants suggested that progress would be enhanced through network management and standardization. During discussion of network management, participants focused on the growing complexity of the telecommunications networks. They suggested that solutions would likely evolve from using modeling and simulation and testbeds to developing pilot programs and testing forthcoming technologies. To properly test future technologies, participants discussed the need to develop dynamic models. They stated that such models were needed to give assessments of the present state of the network, as well as to model the network with changing technologies within the various system layers. Ultimately, participants stated that systems analogous to GETS that used innovative technologies to provide priority service across all channels needed to be tested and prototyped.

4.5.2 Priorities for Research Integration

The challenge remains as to how to drive technology innovation into NS/EP systems and functions. The complexity derives from the lack of an overall system architecture that incorporates trust in each system layer, starting from devices, components, systems software, and working through all the applications layers. Research needs to be vertically integrated across these layers and mechanisms developed to identify and integrate technologies related to trust.

During their discussions, participants determined that specific types of collaborations among industry, Government, and academia were needed to successfully integrate NS/EP systems. They noted how NS/EP telecommunications utilized a commercial infrastructure and that Government lacked sufficient leverage to impose its requirements due to its diminished "purchasing power." Some participants noted that industry often lacked detailed insights into what requirements were needed to support critical Government services and questioned who from the Government would pay for the development of enhanced services. They also emphasized that Government should understand that its standards and requirements might be unique and not implemented across the network because they would offer little commercial value or revenue. Participants noted that additional research was needed to determine the policy implications of requiring different applications and services from the industry standard infrastructures to support national security requirements. Reliance on the private sector market requires that Government, in designing NS/EP systems, be aware of international and global developments and be prepared to cooperate and collaborate to assure global integration.

Participants also discussed the development of new economic incentives for industry to participate fully in Government R&D initiatives. They stated that Government programs needed to be sensitive to economic incentives to encourage market driven industry to experiment with innovative technologies that can be successfully implemented in future NS/EP systems.

4.5.3 Impediments to Research Integration

Participants noted that a major impediment to research was the weak market for assurance products and services. They stated that revenue conscious firms had little incentive to prioritize innovations in trustworthiness and that the commercial infrastructure that supported NS/EP operations and services units was under short-term revenue pressures. Moreover, many of the larger telecommunications companies lacked a culture of conducting applied research and that only recently had academia and Government begun to look seriously at the technological challenges in those areas.

Participants stated that the challenge was attracting the operations elements of industry to provide resources and assets, including most importantly people, access to real systems, and funding to conduct tests in collaborative and innovative research projects, pilots, and testbeds. They commented that economic incentives needed to be created for all sectors to cooperate and interoperate on R&D.

Participants observed that Government funding was a critical component to success in trustworthiness, but it was not the overriding factor. They stated that the most important factor was adopting an R&D strategy that would attract participation from all the technology, industry, and user sectors to drive the integration into the real systems. Consensus on the unprecedented

needs and capabilities indicates a need for rapid prototyping and testbeds to assure the desired integration into future NS/EP systems.

Some specific R&D challenges discussed included: providing for underlying system recovery and restoration from catastrophic failure; determining which functions could be performed from backup mode; and as NS/EP capabilities became more pervasive and embedded in the internetworking, a need to build IT forensic science for assured systems.

4.5.4 Path Forward

For success in achieving trustworthiness, participants emphasized that need to develop a research agenda and strategic approach to implement NS/EP R&D programs across industry, Government, and academia to leverage advances in all sectors in information technologies and impact across the standards development process in information assurance technologies. Participants discussed how to initiate or use existing testbeds to fully stress models on emerging innovative systems that would include wireline, wireless, ground-air systems and to safely test and qualify technologies. They noted that prototyping testbeds allows scalable approaches to achieving trustworthy systems that are capable of being configured for a wide range of end-user configurations and threat models. This will promote the transition of functionalities into the existing Internet technology base as system trustworthiness is attained by all participating sectors.

More specifically, participants discussed how potential improvements for existing levels of technologies could be advanced by making end user authentication at the edges, securing the channel, and improving reliability of the channels and priority mechanisms.

Participants suggested that new systems could include the full range of internetworking functionality to enable dynamic collaboration among a wide range of end users and their systems. They also offered that such an approach should include advanced collaborations for a wide range of devices along with advanced services and modeling and simulation for decision analysis. They stated that such prototype systems would be viewed as a highly enhanced secure version of the evolving Internet.

Participants noted that promising strategies included investment in additional technologies to supplement bandwidth. They stated that a likely area was IPv6, which enabled enhanced security. Participants added that such systems would need to be tested in cases where virtual information resources were allocated dynamically to create the IT resources needed for extraordinary requirements for critical NS/EP situations. Some of the ideas that were discussed included general peer-to-peer systems structures to enable interaction and integration of resources and functions. A prerequisite for such tests would be the expansion of threat scenario models to include new vulnerabilities and threats that were relevant to the new functionalities.

Participants also discussed the issue of threat analysis, debating the amount of risk NS/EP telecommunications systems could bear before being deemed too vulnerable. They suggested that current threat scenario models could be expanded to include the introduction of new vulnerabilities and threats that would keep pace with changes in technology and functionality in telecommunications networks and the Internet. Participants emphasized that threats were extremely dynamic and required constant attention and suggested examining threat issues from the standpoint of vulnerabilities as opposed to defined threat scenarios.

Participants suggested that the NS/EP user community could be organized into systems and groups based on acceptable threat levels. They also focused on the development of solutions based on past experiences with threats. Participants suggested examining regular outages and disaster recovery responses to gain knowledge and understanding of how systems worked under duress. They noted that such responses could be mirrored and applied in the NS/EP telecommunications arena.

5. CLOSING PLENARY SESSION

The closing plenary of the R&D Exchange began with presentations from the facilitators from each breakout session. Following those briefings, Dr. Marburger concluded the exchange by summarizing the four overarching themes from the presentations. The four themes are:

- Clarifying and qualifying threats is a crucial variable in helping the private sector to better identify and understand the vulnerabilities most likely to be exploited. A more precisely defined and prioritized set of threats (e.g., the capabilities likely to be employed by bad actors against NS/EP telecommunications) could help rationalize both public and private investments in specific technologies designed to eliminate or reduce the potential impact of vulnerabilities;

- Documenting, mapping, modeling, and analyzing existing systems is beneficial for better understanding key points of failure, anticipating how integrating new technologies/applications might introduce new vulnerabilities, and assessing the potential impact (both direct and indirect) of system failures;

- Developing improved technologies, tools, and techniques is needed to help owners and users better monitor, analyze, and learn from network incidents so that they can better determine how successful cyber attacks are conducted; and

- Addressing the current political and bureaucratic processes that appear to be delaying previous recommendations from being acted upon is necessary.

The participants agreed on the need to frame the problem as a project, focusing on the major steps, priorities, milestones, and capabilities needed to successfully start to embed trustworthiness in emerging, current, and legacy systems. Dr. Marburger emphasized the need to have an overarching framework for the trustworthiness issue that included an action plan and associated roles and responsibilities for industry, Government, and academia. To facilitate increased public and private funding, he stated that developing measures for cost effectiveness and return on investment was crucial. Concluding his remarks, Dr. Marburger commented that he was quite optimistic that industry, Government, and academia could successfully collaborate to extricate themselves from a cycle of repeating recommendations. With the development of DHS, he said the U.S. Government should have a clearer focus and lines of responsibility for dealing with current and emerging R&D issues.

6. EXCHANGE FINDINGS

The R&D Exchange 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, six issues regarding the trustworthiness of NS/EP telecommunications and information systems emerged:

- **A strong sense of frustration and urgency.** Participants noted the R&D Exchange was but one of many conferences and events focused on issues of trustworthiness and security. They commented that each event produced similar results and recommendations, but that action and implementation were fleeting. At the same time, however, they conveyed a strong sense of urgency about trustworthiness topics. Participants agreed that, given the global nature and increasing proliferation of distributed denial of service attacks and computer viruses, grappling with how to prevent and mount effective responses to such types of attacks was a pressing national issue requiring senior-level attention and commitment in industry, Government, and academia.

- **A need to identify and clarify the definition of NS/EP telecommunications in the post 9/11 world.** An issue frequently discussed at the event was the changing nature of NS/EP telecommunications. Participants noted that the changing threat environment (from Cold War to distributed threats posed by rogue states and international terrorist groups), evolving technologies (from the traditional public switched network to a converged network composed of traditional voice services, wireless services, the Internet, etc.), and creation of new Government institutions (the Department of Homeland Security) all generated a need to clarify the meaning of NS/EP telecommunications in the post-September 11th environment. They also agreed that a better understanding of NS/EP telecommunications might serve as a catalyst for, and offer a rationale for, prioritizing R&D in key security technology areas.

- **A need to address major challenges on driving technology innovation into NS/EP systems and functions.** The complexity associated with driving technology innovation into NS/EP systems and functions derives from the lack of an overall system architecture that incorporates trust in each system layer, starting from devices, components, systems software, and working through all the applications layers. Research needs to be vertically integrated across these layers and mechanisms developed to identify and integrate technologies related to trust. Consensus on the unprecedented needs and capabilities indicates a need for rapid prototyping and testbeds to assure the desired integration into future NS/EP systems.

- **A need to establish partnerships for R&D integration.** Government funding is a critical component to success in trustworthiness, but it is not the overriding factor. The most important factor is adopting an R&D strategy that will attract participation from all the technology, industry, and user sectors to drive the integration into the real systems. The challenge is to attract the operations elements of industry to provide resources and assets, including people, access to real systems, and funding to conduct tests in collaborative and innovative research projects, pilots, and testbeds. Economic incentives need to be created for all sectors to cooperate and interoperate on R&D.

- **A need to influence business drivers for security.** Historically, public research was the primary driver for technology innovation and development in the United States. During

the Cold War, the research community relied in the main on U.S. Government funding and direction. In the 1990s, however, this model evolved with private funding of research and technology development equaling and exceeding Government investment. Recognizing the shortage of available resources (Government R&D funds and grants, capital investment in industry, budget cutbacks at universities), participants discussed the need to collaborate on ways to stimulate and leverage market forces as a catalyst for developing the next generation of security tools and products.

- **A need to improve threat definition and analysis and, equally important, identify methods to share and analyze that information to influence R&D.** Participants agreed that understanding the evolving capabilities and intent of potential adversaries (nation-states, terrorists, hackers, insiders) was an important element in developing security tools and products that would meet the future needs of industry, Government, and academia. Participants noted that it was crucial to future R&D to develop a baseline of existing telecommunications and computer networks and to invest in enhancements to the Internet that would allow for regular and more real-time monitoring, modeling, simulation, analysis, and testing of new vulnerabilities.

- **A need to strike a better balance between better engineering of software and hardware with efforts to improve human factors.** Participants noted the importance of having a well-trained and educated workforce, consistent and enforced policies, and a better understanding of what motivates and deters insiders, and how they accomplish intrusions. A concern regularly expressed at the event was that every action taken in one realm (cyber, human factors, physical, integration) had both visible and often hidden impacts on the other.

APPENDIX A: AGENDA

APPENDIX A. AGENDA

Thursday, March 13, 2003

10:00 – 12:00 p.m.	Plenary Session
10:00 – 10:05 a.m.	Welcome/Introduction – Dr. Seymour Goodman, Professor of Computing and International Affairs, Georgia Tech, and Co-Director, Georgia Tech Information Security Center
10:05 – 10:15 a.m.	Welcome/Introduction of Keynote Speaker – Dr. G. Wayne Clough, President, Georgia Tech and Member of the President's Council of Advisors on Science and Technology (PCAST)
10:15 – 10:45 a.m.	Keynote Address – Dr. Marburger, Director, Office of Science and Technology Policy
10:45 – 11:00 a.m.	NSTAC's Perspective – Mr. Guy Copeland, Vice President, Information Infrastructure Advisory Programs, Computer Sciences Corp.
11:00 – 12:00 p.m.	Introduction of Breakout Sessions – Session Facilitators
12:15 – 1:15 p.m.	Lunch
12:30 – 12:35 p.m.	Introduction of Luncheon Speaker, Mr. Brenton Greene, Deputy Manager, National Communications System
12:35 – 1:00 p.m.	Luncheon Presentation – Mr. F. Duane Ackerman, Vice Chair, NSTAC, and Chairman and CEO, BellSouth
1:30 – 5:30 p.m.	Breakout Sessions on Cyber/Software, Human Factors, Physical Security, and Integration Issues

Friday, March 14, 2003

8:30 – 10:00 a.m.	Breakout Sessions Continue
10:00 – 10:15 a.m.	Break
10:15 – 12:00 p.m.	Roundtable Plenary Moderated by Dr. Marburger
10:15 – 11:00 a.m.	Facilitator Reports on Breakout Sessions
11:00 – 11:40 a.m.	Question and Answer Period
11:40 – 12:00 a.m.	Closing Remarks – Dr. Marburger and Mr. Copeland

APPENDIX B: ATTENDEES

APPENDIX B. ATTENDEES

F. Duane Ackerman	BellSouth
Peter Allor	ISS
Guy Almes	Internet2
Dimitri Alperovitch	Georgia Tech
Richard Barke	Georgia Tech
David Barron	BellSouth (Facilitator)
James Bean	Verizon
James Douglas Beason	Los Alamos National Labs
Shawn Bilak	SRA International
Clifford (Trey) Blalock	EarthLink
Susan Brenner	University of Dayton
Rick Brown	Georgia Tech
Shelly Brown	Booz Allen Hamilton
Ronald Byrnes	Army Reserve CIO
Scott Charney	Microsoft (Facilitator)
William Cheswick	Lumeta
Ricardo Chiarella	Department of State
Melvyn Ciment	Ciment Consulting
Russ Clarke	Georgia Tech
G. Wayne Clough	Georgia Tech
Shawn Cochran	BellSouth
Guy Copeland	CSC
John Copeland	Georgia Tech
Jim Craft	Raytheon
Stephen Crocker	Shinkuro
Geoff Cumbus	US Secret Service
Lisa Daly	Department of Homeland Security/National Communications System
Ricky Daniels	SRA International
Richard DeMillo	Georgia Tech
Bill Doll	Joint Warfare Analysis Center
Tom Donahue	Central Intelligence Agency
Jon Eisenberg	NRR/Computer Science and Telecommunications Board
Sheree Elliott	Georgia Tech
Heather Ellis	Georgia Tech
Don Erbschloe	U.S. Air Force
Martha Farley	Georgia Tech
Richard Farnham	eCommSecurity
James Fernandez	Georgia Tech
Larry Finkelstein	Northeastern University
Peter Fonash	Department of Homeland Security/National Communications System
Barbara Forrest	Department of Homeland Security/National Communications System
Scott Freber	Northrop Grumman
Peter Freeman	National Science Foundation

Adam Golodner	Dartmouth College
Seymour Goodman	Georgia Tech
James Gosler	National Security Agency
Tim Grance	National Institute of Standards and Technology
Lawrence Greenberg	The Motley Fool Inc.
Brenton Greene	Department of Homeland Security/National Communications System
Joan Grewe	MCI
John Grimes	Raytheon
Onastasia Gunlogson	Unisys
Gerald Harvey	Lockheed Martin
Pam Hassebroek	Georgia Tech
Alaina Hatcher	Department of Homeland Security/National Communications System
Poonam Hattangady	Georgia Tech
Ben Hawkinson	Booz Allen Hamilton
Suzy Henderson	SBC
Conrad Hermann	Zone Labs
James Horton	Georgia Tech
David Hosaflook	Booz Allen Hamilton
Rich Houska	Central Intelligence Agency
Robert Hughes	GuardedNet
Christopher "Topher" Hughes	Cisco Systems
Mary Alice Isele	Georgia Tech
Mike Jacobs	SRA International
Janet Jefferson	Department of Homeland Security/National Communications System
Dan Johnson	Computer and Communications Industry Association
Shirlan Johnson	Georgia Tech
Michelle Keeney	U.S. Secret Service
Shannon Kellogg	ITAA (Facilitator)
Terrence Kelly	RAND
Hank Kluepfel	Science Applications International Corporation
Eileen Kowalski	U.S. Secret Service
Heather Kowalski	Raytheon
Paul Kozemchak	Defense Advanced Research Projects Agency
Jeff Krug	Georgia Tech
Mark Kusiak	Veridian
Phil Lacombe	Veridian (Facilitator)
Susan Landau	Sun Microsystems
Carl Landwehr	National Science Foundation (Facilitator)
Doug Langley	BellSouth
Marc LeBlanc	Office of Science and Technology Policy
Rosemary Leffler	SBC
Steve Lines	Science Applications International Corporation
Dick Lipton	Georgia Tech
Robert Liscouski	Department of Homeland Security
Jon Lofstedt	Qwest

Anthony Love	U.S. Army
Erin MacDougall	Booz Allen Hamilton
Dana Madsen	Central Intelligence Agency
John Marburger	Office of Science and Technology Policy
Scott Marcus	Federal Communications Commission
Gerald Masson	Johns Hopkins University
Maneck Master	Telcordia
Frances Mazzocchi	U.S. Army
Harvey McLaughlin	U.S. Secret Service
Dennis McLynn	BellSouth
John McNulty	Secure Computing
Roberto Medrano	PoliVec Inc.
Christopher Messer	Georgia Tech
Kiesha Miller	Department of Homeland Security/National Communications System
Stephen Mosier	University of North Carolina – Charlotte
William Mularie	Telework, Inc.
Sivaram Muthuswami	Georgia Tech
Mike Nelson-Palmer	Georgia Tech
Son Nguyen	Army Research Laboratory
John O'Connor	Department of Homeland Security/National Communications System
Jack Oslund	George Washington University
Luke Ott	Delta Airlines
Frank Palumbo	U.S. Government Services Administration/Federal Technology Service
David Papas	Secure Computing
Dimitria Papavitch	Georgia Tech
Richard Pethia	Carnegie Mellon
Michael Petry	WorldCom Inc.
Charles Pfleeger	Cable and Wireless
Kevin Piekarski	Department of Homeland Security/National Communications System
Thomas Pilch	Georgia Tech
Marshall Potter	Federal Aviation Administration
Colin Potts	Georgia Tech
Max Poux	U.S. Secret Service
N. Radhakrishnan	U.S. Army
Victor Raskin	Purdue University
Marisa Reddy	U.S. Secret Service (Facilitator)
Robert Roberts	Institute for Defense Analysis
James Romlein	MIS Labs
Robert Rosenstein	Computer Emergency Response Team/Software Engineering Institute
Alberta Ross	Department of Homeland Security/National Communications System
Sue Rosser	Georgia Tech
Marek Rusinkiewitz	Telcordia Technologies

Anthony Rutkowski	VeriSign Inc.
Marshall Sanders	Level 3 Communications
Sami Saydjari	Cyber Defense Agency (Facilitator)
Pat Scherzer	BellSouth
Phyllis Schneck	eComm Security
Corey Schou	Idaho State University
Chad Sellers	Georgia Tech
William Semanic	National Security Agency
Greg Shannon	System Detection, Inc.
Brian Shaw	National Intelligence Council
Annalisa Sheelar	Booz Allen Hamilton
David Shinberg	Lucent
Monique Shivanandan	BellSouth
Bill Smith	BellSouth
Christopher Smith	U.S. Secret Service
Dejan Sobajic	EPRI
Kevin Soo Hoo	@Stake
Stephen Squires	Hewlett-Packard (Facilitator)
Rodney Stalker	Naval Research Laboratory
Victoria Stavridou	SRI International
George "Chip" Stewart	Georgia Tech
David Sulek	Booz Allen Hamilton
Bill Szymansik	National Security Agency
Boleslaw Szymanski	Rensselaer Polytechnic Institute
Cornelius Tate	U.S. Secret Service
William Thomas	Naval Surface Warfare Center – Dahlgren
Lowell Thomas	Verizon
Mary Claire Thompson	Georgia Tech
Michael Vatis	Institute for Security Technology Studies and Institute for Information Infrastructure Protection (Facilitator)
Pamela Warren	Nortel Networks
Jody Westby	The Work-IT Group
James Whittaker	Florida Tech
Diana Williams	National Security Agency
G. Rick Wilson	National Security Agency
Richard Wilson	Office of the Secretary of Defense
Dan Wolf	National Security Agency
Robert Wright	BellSouth
Heather Wyson	BITS
Yi Zhang	Georgia Tech

APPENDIX C: KEYNOTE ADDRESS

APPENDIX C. KEYNOTE ADDRESS

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE
R&D Exchange
Atlanta, Georgia
March 13, 2003

Dr. John Marburger
Director, Office of Science and Technology Policy
Executive Office of the President

Thank you Wayne [Clough] for that kind introduction. OSTP is pleased to co-sponsor this meeting along with the Georgia Institute of Technology. My function this morning is to provide some bureaucratic information. I am relying on this R&D Exchange to help me and my office give guidance to OMB and other White House policy organizations on the need for specific funding or programs to enhance the trustworthiness of the nation's National Security and Emergency Preparedness telecommunications.

Only a few short months ago I was Director of Brookhaven National Laboratory where I was asked to manage a "culture change" in attitudes toward safety and overall conduct of operations. This experience opened my eyes to the need for a holistic, integrated approach to the management of technical systems. This requires systematic input on a regular basis from the people close to the work, who have the experience needed to identify issues that were not taken into account when the systems were initially designed. NSTAC is one of the means for doing that for the nation's NSEP telecommunications systems, and I am grateful for your support.

Before we begin, I want to pause for a moment to reflect on the fact that we are gathering this week at a critical moment in our nation's history. America is preparing to disarm Saddam Hussein and destroy his weapons of mass destruction. More than three hundred thousand coalition forces and nearly a quarter million American troops stand ready in the Persian Gulf should force be necessary. As President Bush stated in his recent weekly radio address, however, "Across the world, and in every part of America, people of good will are hoping and praying for peace. Our goal is peace – for our own nation, for our friends, for our allies and for all the peoples of the Middle East."

Impact of the Creation of the Department of Homeland Security

Here on the home front it is important that our efforts to defend our country are comprehensive and united. The recent creation of the Department of Homeland Security is an important step toward that goal. Earlier this month the new Department began operations in the biggest reorganization of the Federal Government in half a century. The new cabinet-level department ought to make it possible to unify the work of 22 programs and agencies with relevant responsibilities. It is a tool that can provide focus for all the substantial resources of the United States government on the challenging issues of homeland security.

On February 28th the President signed an omnibus of Executive Orders in connection with the transfer of certain function to the Secretary of Homeland Security. Two of the Executive Orders and a new Homeland Security Directive (HSD) are particularly relevant to today's proceedings.

First is Executive Order 12472, "Assignment of National Security and Emergency

Preparedness Telecommunications Functions." One major change introduced by this EO is the designation of the Secretary of Homeland Security as the Executive Agent for the National Communications System. By separate memorandum I have selected Bob Stephan, Special Assistant to Secretary Ridge for Information Analysis and Infrastructure Protection, to be a member of the Joint Telecommunications Resources Board until the President announces a nominee for the Under Secretary position in the Information Analysis and Infrastructure Protection Directorate. Mr. Stephan has also taken on responsibility as Acting Manage for the National Communications System. The Joint Telecommunications Resources Board, for those of you who don't know, serves as a deliberative and recommending body for me, and ultimately for the President, for the provision of necessary telecommunications services, information, and advice.

One other significant change in 12472 is the addition of the Homeland Security Council to the list of those organizations that the National Communications System provides assistance to in the exercise of telecommunications functions and responsibilities. This change ensures coordination of homeland security-related activities. The Homeland Security Council is the new White House policy entity replacing the Office of Homeland Security, which no longer exists. Its role is redefined to accommodate the new Department.

The second Executive Order of particular relevance here is 12382 – the "President's National Security Telecommunications Advisory Committee (NSTAC)." This Executive Order establishes a new reporting mechanism for the NSTAC through the Secretary of Homeland Security to the President. The Office of Science and Technology Policy did not prepare the text of this EO, but I understand that the intent was to ensure appropriate coordination with the Department of Homeland Security. I also understand that the Executive Order continues to show the Secretary of Defense as the Executive Agent for the National Communications System, which is not correct. I have been assured that this error will be corrected later.

Finally, Homeland Security Directive 5 – Management of Domestic Incidents – directs the Secretary of the Department of Homeland Security to develop a National Response Plan that integrates Federal Government domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan. The Directive recognizes the criticality of national security and emergency preparedness by directing the Secretary to consult with me, and other officials within the Executive Office of the President, in developing and implementing the National Response Plan.

Collectively, the amended Executive Orders, the new Homeland Security Directive, along with the other existing Presidential Decision Directives ensure that national security and emergency preparedness telecommunication services will be available in times of crisis for the President, other national leaders, and the emergency preparedness and response community.

Organizing for Results

My confirmation hearing on October 9th, 2001, just a month after the terrorist attacks gave me the opportunity to declare that "the struggle against terrorism has many fronts, and science and technology pervade them all." I believe that, and the nations response since then has confirmed it. In a national security and emergency preparedness era, where voice and data networks are

merging and the next Generation Network is *emerging*, it is ever more critical that our nation's research and development portfolio be responsive to Presidential and Congressional intent, that our programs are well-coordinated, and that our research and development funds are used efficiently.

Our nation's advantage in R&D must be harnessed to support our national security and emergency preparedness telecommunications functional requirements. Survivability/ endurability, reliability/availability, interoperability, and enhanced priority treatment are just a few of the requirements identified by the Convergence Working Group Report of January 2002 as needing special attention. Here, today and tomorrow at this Exchange, the focus will be on trustworthiness, another critical functional area of concern. Your input will be used to help formulate the President's research agenda and an agenda for action.

One tool we use for coordinating R&D among federal agencies and departments is the National Science and Technology Council (NSTC). This is a cabinet level organization with representation by every federal department or agency engaged in R&D activities. Administered by OSTP, the NSTC has four standing committees on Science, Technology, Environment, and Homeland and National Security. Each committee is organized into subcommittees and working groups that are focused on a particular set of issues. We will use the NSTC mechanism for coordinating R&D related to critical infrastructure protection, and we will do it through a subcommittee with dual reporting to the Committee on Technology and the Committee on Homeland and National Security. Working groups will form under this subcommittee to focus on the physical or cyber aspects of infrastructure protection. The subcommittee will rely on

NSTAC for the traditional support it has provided for National Security and Emergency Preparedness R&D issues.

Implementation of a comprehensive critical infrastructure protection R&D plan must include participation from and cooperation among multiple R&D communities: industry, academia, and government. The creation of a National Science and Technology Council subcommittee focused on infrastructure protection issues provides a mechanism for developing an integrated federal R&D agenda responsive to threats to the United States.

The President's FY 2004 Budget Proposal

In my testimony last month before the United States House of Representatives, Committee on Science, I noted that the President has a strong commitment to research and development in the national interest. The President's fiscal year 2004 budget focuses on winning the war on terrorism, securing the homeland, and strengthening the economy. Considering the context of an uncertain economic environment and growing federal deficit, any increase in discretionary spending is difficult to justify to the American people. However, the President's budget requests another record high level of funding for R&D: $123 billion or a 7% increase over the 2003 request. More than $5.9 billion of the increase is in Department of Defense development activities, reflecting the President's commitment to bolster our national defense and homeland capabilities. The overall increase in R&D spending is evidence of the importance this Administration places on science and technology in addressing our country's present and future challenges.

In conclusion, these next two days provide a focused opportunity to explore the research and development issues associated with trustworthy national security and emergency preparedness telecommunications. We must focus because the concept of trustworthiness is very broad, but here the emphasis is on the context of national security and emergency preparedness of telecommunications. Please understand that your work will have a real impact on the President's research and action agendas. I look forward to hearing and reading your conclusions, and wish you an enjoyable and productive exchange.

Thank you.

APPENDIX D: LUNCHEON PRESENTATION

APPENDIX D. LUNCHEON PRESENTATION

From the Moth to the Worm: Ensuring Networks That Keep America Safe and Strong.

Remarks by F. Duane Ackerman, Chairman and Chief Executive Officer, BellSouth Corporation to the National Security Telecommunications Advisory Committee (NSTAC) Research and Development (R&D) Exchange, Atlanta, Georgia, March 13, 2003.

Thank you, Brent [Brenton C. Greene, Deputy Manager, National Communications System].
Good afternoon. On behalf of NSTAC and BellSouth, I'm pleased to welcome you to Atlanta. And, I want to thank you for making this journey and for the important work you are doing to ensure the trustworthiness of the critical networks that keep America safe and strong.

I want to thank Dr. John Marburger [Director, White House Office of Science and Technology Policy) for joining us. The President has made it very clear that research and development are critical components of the war on terrorism, and so I want to thank Dr. Marburger and his team for keeping innovation front andcenter on our national agenda.

I also want to thank my friend, Dr. Wayne Clough, and the Georgia Tech community for hosting this event. We are very proud in Atlanta to have one of the nation's top research universities in our city. You know, Georgia Tech students are famous for their serious work ethic, but they also know how to have fun. I hope you'll catch that spirit while here and enjoy some of our southern hospitality.

NSTAC'S Mission in a Changing World

The people in this room represent the central nervous system of our nation's infrastructure. The state of that system is strong. At the same time, it has never been more vulnerable.

Network technology has delivered new powers to American consumers and businesses, driving costs down and increasing productivity. Our unprecedented connectivity has become one of our greatest competitive strengths—but it has also become one of our greatest weaknesses.

As we gather to explore the trustworthiness of our systems, let me share a few historical snapshots, courtesy of the Washington Post, that I believe symbolize the challenge before us:

- In 1945, Rear Admiral Grace Murray Hopper and her team discover a moth…yes, a moth… trapped between relays in one of the earliest Navy computers. They remove it with a pair of tweezers and Admiral Hopper coins the term "debugging" to describe efforts to fix computer problems.
- In 1972, John Draper, subsequently known as "Captain Crunch," discovers that the plastic whistle in a box of cereal reproduces a 2600-hertz tone. With a "blue box" tone generator, the pioneer hacker unlocks AT&T's phone network, allowing free calls and manipulation of the network.
- In I998, intruders infiltrate and take control of more than 500 military, government and private sector computers. The incidents were thought to have originated from operatives in Iraq. Investigators later learn that two California teenagers were behind the attacks.

- In January 2003, the "SQL slammer" worm infects hundreds of thousands of computers in less than three hours. The fastest-spreading worm ever wreaks havoc on businesses worldwide, knocking cash machines offline and delaying airline flights.

A universe of change lies between the moth in the machine and the worm in cyberspace.

We're making the leap from the machine age to the systems age. Physical assets are converging with digital assets. Networks are converging with computers. Our critical economic and governmental operations—from communications to banking, energy and transportation—now depend on information systems and the nearly two billion miles of cable and switches that connect them. Today, we are all linked by a stream of ones and zeroes. Like most major telecommunications providers, BellSouth has a long history in cooperating with national, state and local officials to address issues of trustworthy networks, national security and emergency preparedness. And we take pride in this partnership.

In the same way, participation in NSTAC is vital to us because we are committed to keeping the phones ringing and the ones and zeroes flowing for the nation…and our 44 million customers, including many critical infrastructure providers and first responders. Together, we have kept people connected through hurricanes, floods, fires and ice storms. One of the most telling images I remember seeing in the Southeast was some footage shot during Hurricane Andrew. It showed an area of utter devastation, houses split open, cars turned upside down. But in the foreground, a person is talking on a BellSouth phone. In the midst of all this destruction, the phones still worked. That's reliability. That's trust.

But now we face new, human risks—from the teenage hacker probing for holes in the network to the malicious terrorist seeking to disrupt and destroy. Mother Nature has been joined by man-made threats, like cyber attacks, truck bombs, chemical, biological and even nuclear events.

The stakes for the nation and our customers have never been higher…our collective work through NSTAC never more important. From the NSTAC perspective, our fundamental mission remains the same: first, to prevent an attack and protect our national security—and that means both physical and cyber security—and second, to be prepared to respond when an emergency strikes. But how we carry out that mission has become increasingly complex.

There is a growing disconnect between the pace of technology and our ability to manage it. Policies that control the telecommunications industry were written for an earlier age and discourage investment in R&D when we need it most. And network speed and connectivity require a new level of partnership.

How we ensure trusted networks and systems must change as technology evolves. Yesterday it was the moth and Mother Nature. Today it's also worms and viruses unleashed by man. What threat—and opportunity—will we face tomorrow? The central nervous system—we who develop, operate and regulate those trusted networks—will need to bridge the widening gap between the state of our technology and the state of our management.

We Must Do Three Things

I'd like to touch on three issues that, from our perspective, will affect our ability to ensure trusted networks. The first has to do with how we manage security and emerging technology. The other

two have to do with non-technical but fundamental factors that will determine how well we manage our trusted networks—public policy and partnership.

First issue: We need R&D to help us manage security as technology evolves. Private industry owns and operates nearly 90 percent of the nation's critical infrastructure. But, private industry has always depended on public science to fuel innovation. In the decade ahead, we will spend billions of dollars to protect and upgrade our networks and systems. And now more than ever, we need cutting edge R&D to make sure that we are spending those dollars wisely.

Physical security around "guns, gates and guards, " is a vital part of the security strategy. We need R&D in new areas like identity management and access control. I think it is safe to say the policy of this country for the last decade or so has been to open networks, open buildings, open interfaces in our communications networks. There are people with access to some of the most sensitive infrastructure locations in the country and we don't know who they are.

Research needs to examine the possibility of creating a standard system of national security background checks and identity verifications to help ensure that only authorized personnel are getting access to critical facilities. The availability of an interoperable standard for tamper proof, certificate based ID cards might help in this area. Technology like biometrics could be considered to ensure the identity of a card.

Today, security means better physical security, but it also has to encompass cyber security. The challenge here is that network technology is outpacing our ability to manage it. We spent decades developing finely-tuned management practices in our existing networks. And we certainly need to keep mastering the fundamentals—documented policies, defined response procedures, disaster recovery and business continuity, redundant designs, fail-over architectures and ongoing audits. But beyond these fundamentals, there are important opportunities for R&D in evolving our network management techniques to keep pace with emerging technology.

We need a national strategy for continually hardening our existing network against attacks, and at the same time adapting new types of networks and protocols to ensure the same trust in new infrastructure as in the existing public switched network. By "new infrastructure" I am talking about that place where the Internet has converged with our public switched network. The next-generation networks like MPLS and new protocols like IPv6 bring with them a host of new capabilities as well as a host of new issues. Emerging networks require new operating support systems and control systems to ensure their operability and security.

Let me elaborate a little more…

First: we need to secure the network…in other words…make it hard for the worm to get to us.

The sheer complexity of today's communications infrastructure introduces security exposures. There are over a billion access points to the Internet. A physical connection actually exists between the most determined terrorist organization on one of these access points and the most sensitive network system.

From a research perspective, the critical areas to consider are the network management interfaces, the security of the protocols that are involved in managing the connections and

transporting information, and the assurance that the software configurations deployed actually match the intended configurations and have not been intentionally or unintentionally altered. It is critical that we reduce the number of vulnerabilities in the infrastructure through better software development. Many exposures have been introduced through coding errors during the development process. Security implications should be considered in the earliest stages and throughout the development process.

R&D is also required to improve the security of wireless networks so that these technologies can be confidently integrated into the infrastructure.

Second, we must "detect and defend" the network … notice when the worm attacks and quickly block the attack.

Not all attacks will be prevented. So we need mechanisms to automatically detect and quickly respond to attacks. Standard techniques are based on monitoring traffic at network endpoints. Research into further techniques here would help, but most importantly we need more research in network-wide pattern recognition and attack detection.

Service providers need to be able to see overall traffic patterns across many ports in the network rather than seemingly random events from a single network end point.

We need detection in the face of secure tunnels and tunneling protocols—not just cryptology, but detection based on packet flow patterns. Also controls to proactively shut down interfaces or restrict certain types of traffic when attack patterns are detected.

Third, the network needs to adapt and survive—so that if a worm gets through, the network may be injured, but it will not collapse.

We cannot control every access point in cyberspace. Redundancy of network capacity and connectivity, along with network management techniques play a key role in the survivability of the network.

But we can also create a more trusted cyber-environment through separate identifiable network domains by using traffic priorities, Quality of Service capabilities, and Virtual Private Network technologies. This would ensure that the most critical traffic continues to flow when natural or malicious events unexpectedly force major reroutes of network traffic.

These are just a few of the areas that need focus from our perspective, but as you know, I'm just skimming the surface here. Keeping America safe and strong will require massive investment in innovation and R&D, which brings me to my second issue and it has to do with policy.

Second issue: Policymakers must realize that we cannot have Homeland Security without Economic Security. I have to tell you that when I think about network security today, I worry more about the incoherent state of telecommunications policy than I do about technology or terrorists. One of the greatest national security risks our industry faces today is investor uncertainty, which leads to the question of how our networks will be financed in the future.

Our best defense — and offense —against an attack rests with the industry's ability to invest in our core data networks. We must be able to provide redundant network capacity to protect against physical and logical failures, so that we can increase network management and security.

So that we can deploy networks that support Quality of Service and Virtual Private Network capabilities to guarantee that attacks and incidents in one part of the network don't interfere with other parts of the network.

In our increasingly data-centric network environment, R&D spending plays a critical role in improving the price, performance, management, and security of network equipment. So that carriers can, through increasingly efficient use of bandwidth, transmit ever-larger volumes of data traffic at ever lower costs with ever increasing reliability.

And yet, at a time when we need to invest more, capital spending in the telecommunications industry has collapsed because of economic and regulatory uncertainty. Capital expenditure in telecom is expected to fall another 17 percent this year and remain flat through 2005.

In the 20th century, our nation led the world in the deployment of advanced telecommunications infrastructure. Americans prospered from a steady flow of innovation, with better ways to get our work done, to learn, to create, to produce, to raise our standard of living.

Prosperity and security together form the backbone of America's strength. Will we unleash a new wave of investment and innovation? Or will we let our national infrastructure fall behind?

I encourage all of us, including our partners in academia, to work on developing public policies that will help restore and protect the financial integrity of our national networks as we adapt to new threats and rapid technological change.

Third issue: In the Age of Networks, Security and Trust Depend on a Network of Partners. Terrorists and cyberspace know no boundaries. Neither can our response to this changing world. We cannot operate in isolation. As technology expands, so does the range of stakeholders. Where do we find common ground…common standards and priorities? Where are the points of intersection? What are the Best Practices? How do we strike the right balance between sharing information and protecting our proprietary interests? Between infrastructure security and scientific openness?

The concept of trustworthiness will evolve as new technology emerges. The moth corrupted a single computer. The worm in cyberspace endangers us all.

Maintaining "trusted" networks to stand up under all conditions and attacks will require an even stronger network of partners.

At its heart, NSTAC is a learning and teaching organization, giving us access to the thinking of the best and the brightest to help us better serve the nation and our customers.

You've done a lot of listening this morning. Now it's your turn to think and talk through the critical R&D issues we face around security and technology in the telecommunications sector. Your work is urgent. The needs are real. Your talent is deep. And I look forward to the output from your exchange.

The President has said, "The terrorist enemy we face is highly determined, patient and adaptive. In confronting this threat, protecting our critical infrastructure and key assets represents an enormous challenge. We must remain united in our resolve, tenacious in our approach and

harmonious in our actions to overcome this challenge and secure the foundations of our nation and way of life."

We are the central nervous system of our nation's infrastructure. We are its lifelines. We all represent key organizations and bring unique and diverse experiences to this task.

But when it comes to our role in NSTAC, there is only one agenda. Keeping America strong. Keeping America safe. Keeping America connected.

And, as Tom Ridge has said… Keeping America prepared and ready.

Thank you for doing your part.

APPENDIX E: BREAKOUT SESSION BRIEFING SLIDES

APPENDIX E. BREAKOUT SESSION BRIEFING SLIDES

The President's National Security Telecommunications Advisory Committee

2003 Research and Development Exchange Breakout Session Briefings

March 14, 2003

The President's National Security Telecommunications Advisory Committee

R&D Exchange Cyber/Software Breakout Session 1

Mr. Scott Charney, Microsoft
Mr. Phil Lacombe, Veridian

March 14, 2003

Cyber/Software: Current State of Trustworthiness

The group believes that the Office of Science and Technology Policy (OSTP) should focus R&D efforts around three main areas:

- **Short-term research activities that could improve the trustworthiness of software and cyber systems in the near future**
- **Long-term research activities that could embed the concept of trustworthy computing in the design of future systems**
- **Policy issues that either promote or impede the development and deployment of secure and trustworthy cyber systems**

Cyber/Software: Technology To Improve Trustworthiness

Short-term cyber security research priorities should focus on:

- **Economic incentives for developing and deploying secure technologies**
- **Develop methods and tools to eliminate vulnerabilities in the development process**
- **Secure protocol design and development; analyze current routing and signaling protocols**
- **Improving security in legacy systems**
  - **Testing techniques for finding vulnerabilities in existing software and Infrastructures**
  - **Validation and quality assurance of patches**
- **Priority routing in all networks during emergency response with assured quality of service**
  - **Modeling and simulation mechanisms to identify key telecommunications uncovered circuits**
- **System-wide recovery and remediation**
- **Detecting systems' state and developing intelligent systems that measure and monitor incoming/outgoing traffic; configure personal firewall settings automatically; and provide automated policy development, deployment, and enforcement**
- **Understanding what information needs to be shared among infrastructure providers**
- **Promoting risk assessment studies that analyze costs of implementation and consequences of insecurity**
- **Develop a methodology to validate best practices and apply that methodology**

Cyber/Software: Impediments to Future R&D on Trustworthiness

Long-term cyber security research priorities should focus on:

- **Support for basic research in the science of cyber security**
  - **Building and deploying inherently secure architectures**
  - **Testing and evaluation of large scale systems**
  - **Identifying the elements of security**
  - **Defining rules of composition for large scale systems**
  - **Defining and developing technical metrics that measure security and strength of security**
- **Security of embedded systems**
- **Computer security embedded measures to reduce software vulnerabilities**
- **Modeling and simulation of networks**
- **Compilers that eliminate or (at least) find vulnerabilities during compilation**
- **Tools development for authentication, forensics, and attribution**

Cyber/Software: Input to the OSTP and the NSTAC

The group identified a list of vulnerabilities that need to be addressed, which formed the context of our discussion:

- **Internet Signaling Gateway effects on PSN**
- **Signaling and Routing Protocols**
- **Peer-to-peer technology**
- **Trustworthiness of code**
- **Wireless**

Cyber/Software: Agenda for Action Gold Nuggets

The group has also identified promising new technologies:

Network Topology projects:

- **GEWIS (Global Early Warning Internet System) is an early warning system using commercially available/provided global data on internet performance based on industry tools.**
- **CERT is developing a similar network traffic flow program to identify security events.**

Cyber/Software: Agenda for Action

R&D cyber security policy recommendations to OSTP:

- **Set the research agenda by focusing on:**
  - **Evolving threats**
  - **Evolving technologies**
  - **The ability to implement the research**
- **Cyber security needs visibility and influence**

The President's National Security Telecommunications Advisory Committee

R&D Exchange
Cyber/Software Breakout Session 2

Carl Landwehr, National Science Foundation
Sami Saydjari, Cyber Defense Agency

March 14, 2003

What we did

- **What we did:**
  - **Scoping discussion**
  - **Desired end states**
  - **Research topics driving to the end states**
  - **Final recommendations/actions**

Research Areas and Assessment

Research Topic	System Decision	Bldg Blocks E&T	Policy	Difficulty	Time Range	Pay-off
Security Metrics. For example, create benchmarking (automated testing/validation) systems publicly available, perhaps as element of certification. Must define trustworthiness from arch/software persective	p	s			H	M H
Graded Adversary Threat Models	p	s		s	M	S M
Figure out where we are most vulnerable; Case studies for threat assessment: scenario development and testing (e.g. of "nightmare" scenario). Purpose to validate national vulnerability assessment, eg	p	s			M	S H
Define criticality, criteria, and tiered criticality model.	p	s			M	M M
Management Science of security aspects (ROI and risk). Determining cost to industry of security features/assurance (in $, time to market, performance, etc.). Cost-effective techniques for achieving (validatable) trustworthy systems	p	s			M	M H
Research in tradeoffs between edge security and internal network security.	p	s			M	S M
Explore develop of national cybersecurity testbed. Simulation mode, to assess attack effects, support training.	p	s			M	M H
Systematic study of application of different exisiting telecomm systems for NS/EP application. We have choices today, but perhaps haven't capitalized on them.	p	s			L	S M
Research in economic models for software vulnerability detection/removal.	p	s		s	M	S H

Cyber/Software: Current State of Trustworthiness

- **NS/EP networks have operated reasonably well in practice in many situations of naturally induced faults, errors and failures, including physical attacks.**
- **Economic conditions can trigger changes in the trustworthiness of the underlying telecommunications and computing fabric of NS/EP systems.**
- **NS/EP managers charged with acquiring and managing network resources often face difficult choices among alternatives and lack a strong rational basis for making decisions affecting system trustworthiness.**
- **Reports of new vulnerabilities in NS/EP networks are dealt with largely through intensive manual response.**
- **NS/EP networks and components are significantly vulnerable to malicious attacks exploiting naturally occurring faults and errors.**
- **NS/EP networks would be significantly vulnerable to sophisticated attacks aiming to insert vulnerabilities or sabotage data integrity.**
- **NS/EP network managers can respond to reports of vulnerabilities and incidents with substantial manual coordination in a period of hours to weeks.**

Cyber/Software: Technology To Improve Trustworthiness

- **Develop a Rational Basis for Information Assurance decision making**
- **Improve Systems Understanding and Control**
- **Develop a Well Trained Workforce for Research and Operation**
- **Improve Trustworthiness of Building Blocks**
  - **Better attribution**
  - **Better damage prevention and limitation**
- **Develop Policy fostering Cooperation, Collaboration, Prosecution**

Cyber/Software: Impediments to Future R&D on Trustworthiness

- **Lack of trained workforce of operators and researchers**
- **Lack of convincing case for R&D funding, failing widespread disaster**
- **Lack of a clearinghouse for information on relevant R&D programs**
- **Difficulty of gaining the benefit of the R&D products (not an impediment to R&D per se, but impediment to achieving more trustworthy systems)**
- **Outsourcing of software/hardware, especially offshore**
- **Inadequate, outdated, non-uniform critical infrastructure standards for minimum security in procurements**

Cyber/Software: Input to the OSTP and the NSTAC

- **Caution regarding potential unintended consequences from achieving some research goals**
  - **Individuals and research projects by nature focus on the problem at hand**
  - **Results that could be beneficial sometimes are lost because of external factors not taken into account**
  - **Need for discussion of potential uses of research to proceed in parallel with the research**
- **Recommend longer term examination of research topic areas by a professionally diverse group such as this one**
  - **Possible continuing involvement via electronic means**
  - **Focus on breakthrough technologies**

Cyber/Software: Agenda for Action

- **Set a national vision for trustworthiness of NS/EP systems**
- **Develop scientifically validated, compelling "national security" case (e.g. simulate scenarios) for the vulnerability of existing NS/EP systems**
- **Advocate to the White House research to realize the vision**
  - **Funding**
  - **Coordination: government and industry**

The President's National Security Telecommunications Advisory Committee

R&D Exchange
Human Factors Breakout Session

Dr. Marisa Reddy, U.S. Secret Service
Mr. Michael Vatis, Institute for Security Technology Studies at Dartmouth College

March 14, 2003

Human Factors: Issues of Interest

- **Prevention: minimizing risk of inadvertent failures and malicious acts**
  - Training and policy development, dissemination, and enforcement
  - Technology solutions (e.g., "secure by default," security templates)
  - Human responses to technical information (e.g., alerts)
  - Anomaly detection
  - Psychology/motivations of insiders
- **Cultural shift**
  - Corporate governance (e.g., accountability, enforcement from top to bottom)
  - Public awareness and education (embracing security from the bottom up)
- **Source of Supply: minimizing risk, given growing dependence of U.S. on COTS**
  - Code checking technologies
  - Self-healing (or self-correcting) technologies
  - Background checks (of individuals and/or companies)

Human Factors: Impediments

- Assumptions about balancing security with …
  - Privacy and other policy concerns
  - Good technology
  - Ease of use
- Identifying key business drivers
- Articulating/quantifying value of security
  - "No matter the sophistication of the technology or its simplicity of use, they create an additional burden (investment or maintenance costs)"
- Addressing legal, definitional, and cultural issues
  - Creating an environment where industry and government share data, report crimes
  - What is the definition of NS/EP in today's context?

Human Factors: Most Pressing Research Areas

- Making Security Easier
  - Leverage knowledge from other disciplines to minimize biases and risks related to information security
  - Enhance decision making under uncertainty
  - Reduce impact of human factors (e.g., number of humans interfacing with key systems) by making security transparent
- Anomaly Detection
  - Research automated tools/techniques to detect anomalies (physical access and cyber) across an entire enterprise
  - Enhance tools to better visualize/refine the outputs from detection system
- Education, Training, and Awareness
  - Educate, train, and increase awareness of security issues (e.g., market research for different demographics)

Human Factors: Most Pressing Research Areas

- **"Insider Threat" Research**
  - Investigate true prevalence of insider incidents
  - Research cultural, psychological, technical, and organizational factors that motivate and deter insiders
  - Research tools and techniques to better combat insider threat
  - Translate insider threat research (existing/ongoing) into useful techniques and policies
- **Supply Source**
  - Explore avenues for distributing tasks for checking source code (possible coordination through Centers of Excellence)
  - Validate distribution processes
  - Prioritize what code needs to be checked

Human Factors: Out of the Box Thinking

- Explore paradigm-shifting research in other sectors (e.g., health care, weather forecasting) that might offer new insights into information security
- Research useable, cost effective, and interoperable multi-layer technologies for authentication and authorization
- Research ways to identify suppliers whose products may pose a threat to NS/EP information systems
- Create a market for security (e.g., tax incentives, certification of companies as secure, public filing)
- Research on offensive tactics and strategies for information security

The President's National Security Telecommunications Advisory Committee

R&D Exchange
Physical Breakout Session

Mr. David Barron, BellSouth
Mr. Jim Craft, Raytheon

March 14, 2003

Physical: Current State of Trustworthiness

The current state of trustworthiness related to the physical security of telecommunications assets is characterized by:

- No defined or government validated threats or adversary attack plan against which to protect facilities
- Inability to protect against all feasible attack techniques
- Difficulty in determining what threats exist with regard to the telecommunications industry
- Lack of widespread understanding and appreciation of the sophistication of threats
- Lack of procedures for protecting companies' human capital during times of attack (need to focus on people not just physical assets)

Physical: Priorities

Members of the physical breakout session defined the following top priorities for further investigation through industry/government partnership(s):

- Undertake simulation for NS/EP events and modeling that includes virtual attack/defense of facilities/networks
- Develop better vulnerability analysis to understand critical single points of failure and interdependencies
- Develop industry standards for and implement a national standard industrial I.D. card that is biometrics based
- Investigate standards for the diversity of critical infrastructure
- Develop a system for the automatic defense of cable routes from "backhoes", etc
- Provide better background checks for people with access to critical facilities
- Develop a process to analyze patterns of facility use (looking for social engineering, data mining, etc)
- Withdraw critical vulnerability information from the public domain

Physical: Technology To Improve Trustworthiness

- "Sim Facility" Simulation (like SimCity Game)
- Modeling that includes virtual attack/defense of facilities/networks
- Modeling of cascading, cross sector and widespread/catastrophic outages
- Biometrics
- Immune building technology to deal with biohazards

Physical: Impediments to Future R&D on Trustworthiness

- **Financial constraints**
  - **Companies/Governments do not have the financial/human resources to protect against every possibility**
  - **Regulatory and other pressures may limit some security investments**
- **Competitive nature of the telecommunications industry**
- **Information sharing**
  - **Making information available to the parties that need it without increasing vulnerabilities**
  - **Government does not explain its need and projected use of highly sensitive industry data**
    - **Industry and Government do not demonstrate mutual trust**

Physical: Agenda for Action

An Agenda for Action should:

- **Define levels of "critical" and determine what telecommunications assets can be considered critical for NS/EP purposes and interdependencies**
- **Determine what threats exist with regard to the telecommunications industry and develop a rapid method for disseminating this information to those in industry who need it**
- **Develop modeling and simulations technology related to protection of those assets deemed critical**

The President's National Security Telecommunications Advisory Committee

R&D Exchange
Integration Breakout Session

Mr. Shannon Kellogg, ITAA
Mr. Stephen Squires, Hewlett-Packard

March 14, 2003

Current State of Integrating Trustworthiness

- Current NS/EP telecommunications are limited to voice wireline systems, using analog technologies going to digital
  - Need to develop NS/EP that interoperates across wireline, wireless, satellite and future innovations
  - Systems can operate independently with full functionality
  - Begin the transition to voice over IP systems of all kinds
  - Network management and standardization will be needed to provide full interoperability among systems and tools
  - Should there be a business version of Government Emergency Telecommunications Service (GETS)?
- Challenge: drive technology innovation into NS/EP systems and functions
  - Modeling, simulations, testbeds, pilots and prototype
  - Need to identify how we can integrate technologies related to trust?
  - Integrating voice over multiple kinds of communications channels
  - What is appropriate architecture?
- Challenge: attract industry and operations elements to provide assets and resources
  - Need economic incentives for all sectors
- Challenge: provide for underlying system recovery and restoration from catastrophic failure
  - Determine if the functions can be performed from backup mode

Promising Technologies To Improve Trustworthiness

- Potential improvements for existing level of technologies:
  - End user authentication at the edges
  - Secure the channel, and
  - Reliability of the channels and priority mechanisms
- New systems will include the full range of IT functionality (internetworking) to enable dynamic collaboration among a wide range of end users and their systems
  - Advanced collaborations for a wide range of devices
  - Advanced services: modeling and simulation for decision analysis
  - Such systems will be viewed as a highly enhanced secure version of the Internet
- Promising technologies
  - Invest in additional technologies to supplement bandwidth
  - IPv6 may enable enhanced security
  - Allocate virtual information resources to dynamically create the IT resources needed for extraordinary requirements for critical NS/EP situations
  - General peer-to-peer systems structures to enable interaction and integration of resources and functions
- Threat scenario model must be expanded to include new vulnerabilities and threats that are relevant to the new functionalities

Policy Impediments

- Need to determine the amount of acceptable risk
- Develop measures for quality of service
- International and globalization cooperation and collaboration
- Reliance on private sector market forces for NS/EP systems
- System have to be redesigned to respond flexibly to emerging threats?

Impediments to Future Integration of R&D on Trustworthiness

- Major impediment is the weak market for assurance (IA)
- NS/EP operations and services units are under short term pressures and lack R&D culture
- Lack of programs for applied research in academia, industry and government
- As the NS/EP capabilities become more pervasive and embedded in the internetworking, we need to build IT forensic science for assured systems (IA)

Integration: Input to the OSTP and the NSTAC

- Future NS/EP systems will be an unprecedented expansion requiring a broad range of solutions
- Develop research agenda and strategic approach to implement NS/EP R&D programs across federal government, industry, and academia
  - Leverage advances in information technologies
  - Leverage standards development in information assurance technologies

Integration: Agenda for Action

- **Initiate or use existing testbeds to fully stress models on emerging innovative systems**
  - **Include wireline, wireless, ground-air**
  - **Safely test and qualify technologies**
- **Develop scaleable approach to achieving trustworthy systems that is capable of being configured for a wide range of end-user configurations and threat models**
- **Leverage technology base**
- **Transition functionalities into the existing Internet technology base as system trustworthiness is attained**

APPENDIX F: SPEAKER AND FACILITATOR BIOGRAPHIES

APPENDIX F. SPEAKER AND FACILITATOR BIOGRAPHIES

F. Duane Ackerman is the Chairman and Chief Executive Officer of Atlanta-based BellSouth Corporation. A native of Plant City, Fla., Mr. Ackerman holds a bachelor's degree in physics and a master's degree from Rollins College in Winter Park, Fla., 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, chief executive officer 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 chief executive officer of BellSouth on January 1, 1997. On January 1, 1998, Mr. Ackerman was appointed chairman and chief executive officer of BellSouth.

In addition to serving as a director of BellSouth Corporation, Mr. Ackerman is also a member of the board of Wachovia Corporation and The Allstate Corporation. His civic commitments include immediate past chair of the Georgia Research Alliance and membership on the board of the Woodruff Arts Center. Mr. Ackerman is the chairman of the national Council on Competitiveness, vice chairman of the National Security Telecommunications Advisory Committee, 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.

Dave Barron is currently Director-Regulatory for BellSouth in New Orleans, Louisiana. In this capacity, he interfaces 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 started his career in 1976 in Jackson, Mississippi, as a Communications Consultant in the Marketing/Sales organization of South Central Bell. He had increasing responsibility in Jackson including Senior Account Executive for the insurance market and Account Manager for Mississippi State Government and the Federal Government (GSA) in Mississippi. While in Sales, David was twice recognized by AT&T for being in the top one percent of sales people in the county.

He was transferred to Birmingham, Alabama in 1986 to be on the South Central Bell headquarters staff for Marketing/Sales. He was responsible for sales promotions, advertising, sales incentives, and compensation for the five South Central Bell states.

Mr. Barron was promoted to Director and transferred to New Orleans, Louisiana in 1987 to be the Staff Manager for Marketing and Sales operations for Louisiana. In that capacity, he directed product development and deployment for Louisiana, managed sales promotion and compensation, and provided general sales/operational support for both field and business office operations.

In 1990, Mr. Barron was transferred to Regulatory and External Affairs in Louisiana as the Director-Regulatory. During his time in Regulatory, BellSouth Louisiana achieved Incentive Regulation; migrated to Price Regulation (which has been enhanced and extended once) and

received the support of the LPSC for three 271 applications, the last of which was approved by the FCC.

In August of 2002, he was appointed to be the BellSouth Corporation representative on the Industry Executive Subcommittee (IES) of the President's NSTAC. David will serve as the Vice-Chairman of IES and will assist Mr. Ackerman in supporting the partnership between the Federal Government and BellSouth in matters involving national security and emergency preparedness. 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.

Scott Charney is the Chief Security Strategist for Microsoft Corporation. He oversees the company's Trustworthy Computing initiative, which aims to promote a safe, private, and reliable computing experience for everyone. Mr. Charney also leads the Security Strategies Group, which works with product teams and others at Microsoft to advance the development of secure products, services and infrastructures through the use of appropriate policies and controls, the implementation of best practices, and the development of useable security products and services. He also collaborates with others in the computer industry and the government to make computing more secure for all users. Mr. Charney's goal is to reduce the number of successful computer attacks and increase the confidence of all users in the security of their personal computer.

Mr. Charney has a wealth of experience in computer security in the private sector and government. Most recently, he was a principal for the professional services organization PricewaterhouseCoopers (PwC), where he led the firm's Cybercrime Prevention and Response Practice. He provided proactive and reactive computer security services to Fortune 500 companies and smaller enterprises.

Before joining PwC, Mr. Charney served as chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division of the U.S. Department of Justice. As the leading federal prosecutor for computer crimes, he helped prosecute nearly every major hacker case in the United States from 1991 to 1999. He co-authored the original Federal Guidelines for Searching and Seizing Computers, the federal Computer Fraud and Abuse Act, federal computer crime sentencing guidelines, and the Criminal Division's policy on appropriate computer use and workplace monitoring. He also chaired the Group of Eight nations (G8) Subgroup on High-Tech Crime, served as vice chair and head of the U.S. delegation to an ad hoc group of experts on global cryptography policy for the Organization for Economic Cooperation and Development (OECD), and was a member of the U.S. delegation to OECD's Group of Experts on Security, Privacy and Intellectual Property Rights in the Global Information Infrastructure. Before working for the federal government, Mr. Charney was an assistant district attorney in Bronx County, N.Y., ultimately serving as a deputy chief of the Investigations Bureau.

Mr. Charney has received numerous professional awards, including the prestigious John Marshall Award for Outstanding Legal Achievement in 1995 and the Attorney General's Award for Distinguished Service in 1998. He was nominated to the Information System Security Association's Hall of Fame in 2000. That same year, the Washington Chapter of the Armed Forces Communications and Electronics Association presented him with its award for excellence in critical electronic infrastructure protection. Among his other affiliations, he served on the American Bar Association Task Force on Electronic Surveillance, the American Health Lawyers Association Task Force on Security and Electronic Signature Regulations, the Software

Engineering Institute Advisory Board at Carnegie-Mellon University, and the Privacy Working Group of the Clinton administration's Information Infrastructure Task Force.

He holds a law degree with honors from Syracuse University in Syracuse, N.Y., and bachelor's degrees in history and English from the State University of New York in Binghamton. Mr. Charney spends some of his free time learning Visual C++® for fun. He also enjoys long hikes in the woods and programming in the Visual FoxPro® database development system.

G. Wayne Clough, Ph.D., is the tenth President of the Georgia Institute of Technology and the first alumnus to serve as president. Dr. Clough received his B.S. and M.S. in Civil Engineering from Georgia Tech in 1964 and 1965, and a Ph.D. in 1969 in Civil Engineering from the University of California, Berkeley. Dr. Clough was a member of the faculty at Duke University, Stanford University, Virginia Tech, and the University of Washington. He served as Head of the Department of Civil Engineering and Dean of the College of Engineering at Virginia Tech, and as Provost and Vice President for Academic Affairs at the University of Washington.

During his tenure as president, Georgia Tech received the Hesburgh Award in 1999, the nation's top recognition for support of undergraduate teaching and learning; and in 2001, it was ranked among the top ten public universities by *U.S. News and World Report*. In 2001, *Black Issues in Higher Education* cited Georgia Tech as the first university to graduate the largest number of African-American engineers at all three levels: Bachelors, Masters, and Ph.D.

Dr. Clough has been recognized for his teaching and research, including a total of seven national awards from the American Society of Civil Engineers. He is one of a handful of civil engineers to have been twice awarded Civil Engineering's oldest recognition, the Norman Medal, in 1982 and in 1996. Other recognitions by the American Society of Civil Engineers include the 1991 State of the Art Award and the 1994 Karl Terzaghi Lectureship. He received the George Westinghouse Award from the American Society of Engineering Education 1986 for outstanding teaching and research. In 1990, he was elected to the National Academy of Engineering. He was awarded the 2001 National Engineering Award by the American Association of Engineering Societies.

In 2001, President George W. Bush appointed Dr. Clough to the President's Council of Advisors on Science and Technology, and he chairs the panel on Federal Research and Development. He is a member of the Markle Foundation Task Force on National Security in Information Age. Dr. Clough's other current service activities include: Chair, Governor's Blue Ribbon Natural Gas Task Force; Executive Committee of the U.S. Council on Competitiveness; and Chair, NAE committee: The Engineer of 2020. He is a member of the Executive Committees of Central Atlanta Progress and the Metro Atlanta Chamber of Commerce, and a Trustee of Georgia Research Alliance. Dr. Clough serves on the Board of Advisors for Noro-Moseley Partners, the southeast's largest venture capital fund, and the Board of Directors of TSYS of Columbus, Ga. He serves as a special consultant to the San Francisco Bay Area Rapid Transit System for ongoing major seismic retrofit operations. For six years, Dr. Clough has been listed among the 100 Most Influential People in Georgia by *Georgia Trend* magazine.

Dr. Clough's interests include technology and higher education policy, economic development, diversity in higher education, and technology in a global setting. He is a civil engineer with a specialty in geo-technical and earthquake engineering. Dr. Clough has published over 120 papers and reports and six book chapters.

Guy L. Copeland is Vice President, Information Infrastructure Advisory Programs, with the Computer Sciences Corporation's Federal Sector, and has over 30 years of communications and network experience. For the past eight years, he has served as the principal CSC resource in support of the National Security Telecommunications Advisory Committee (NSTAC), an organization in which CSC's former CEO, Bill Hoover, and current CEO, Van Honeycutt, have been active. 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.

Additionally, Mr. Copeland is responsible for related program advice for CSC's senior management, program executives and other advisory and industry bodies in which CSC participates. He also serves as CSC's member on the Board of Directors of the Information Technology Information Sharing and Analysis Center (IT-ISAC).

Mr. Copeland joined CSC in January 1988 and served progressively as CSC's Director of Program Management Operations, Director of Implementation and Deputy Project Manager for the Treasury Consolidated Data Network. Later he was the Director of the Network Engineering Center in the Network Integration Division.

He represented CSC for three years on the Board of Directors of the Corporation for Open Systems International. He served as organizing chair for the ATM (Asynchronous Transfer Mode) Workshop '95 for the Communications Society of the Institute of Electrical and Electronic Engineers (IEEE) and was overall co-chair for the 1996 workshop. He is a member of the advisory board for "IT Professional," a new publication of the Computer Society of the IEEE.

Mr. Copeland completed his Army career as the project manager for the Army's portion of the Defense Data Network (DDN). Mr. Copeland is a senior member of the IEEE, the Armed Forces Communications Electronics Association (AFCEA) and served on AFCEA's SIGNAL magazine Editorial Advisors Board from 1984 to 1993.

His other memberships include Eta Kappa Nu (Electrical Engineering Honor Society), Tau Beta Pi (Engineering Honor Society), Army Aviation Association of America (AAAA) and the Association of the United States Army (AUSA). His degrees include: masters of science degree in electrical engineering, University of California, Berkeley, California and a bachelor of science degree in electrical engineering from the University of Wisconsin, Madison, Wisconsin.

Richard A. DeMillo, Ph.D., is the Imlay Dean and Distinguished Professor of Computing at the Georgia Institute of Technology. He is also Director of Georgia Tech's Information Security Center. He returned to academia in 2002, after a career as an executive in industry and government. He was Chief Technology Officer for Hewlett-Packard, where he had worldwide responsibility for technology and technology strategy. Prior to joining HP, he was in charge of Information and Computer Sciences Research at Telcordia Technologies (formerly Bellcore) in Morristown, New Jersey, where he oversaw the development of many Internet and web-based innovations. He has also directed the Computer and Computation Research Division of the National Science Foundation.

Before joining industry during the height of the Internet boom, he was Professor of Computer Sciences and Director of the Software Engineering Research Center at Purdue University. He

also held major faculty positions at Georgia Tech where he was the founding Director of the Software Research Center and a visiting professorship at the University of Padua in Padua, Italy.

The author of over 100 articles and books, Dr. DeMillo's research has spanned several fundamental areas of computer science and includes fundamental innovation in computer security, software engineering, and mathematics. His present research interests are focused on information security and nanotechnology. He is developing hardware-based architectures for trusted computing platforms. He is also working on computing and communication architectures for massively distributed nano-scale components. He is active in many aspects of the IT industry, serving on advisory boards and panels and is a member of the Boards of Directors for several companies.

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

From 1994 to 2000, he was Director of the Consortium for Research on Information Security and Policy (CRISP) at the Center for International Security and Cooperation, with an appointment in the Department of Engineering Economic Systems and Operations Research, both at Stanford University; and as Professor of MIS and a member of the Center for Middle Eastern Studies at the University of Arizona (1981-1999).

Prof. Goodman's research interests include international developments in the information technologies, technology diffusion, IT and national security, and related public policy issues. His areas of geographic interest include the former Soviet Union and Eastern Europe, Latin America, the Middle East, South and Southeast Asia, and southern Africa. His earlier research included the areas of statistical and continuum physics, combinatorial algorithms, and software engineering. Dr. Goodman's current work includes research on the global diffusion of the Internet and the protection of large, international IT-based infrastructures. He has published almost 200 articles and monographs, and given about 300 invited presentations on his research.

From 1970-1981, Dr. Goodman was a professor at the University of Virginia (Applied Mathematics, Computer Science, and Soviet and East European Studies). He was a visiting professor at Princeton University (Mathematics, and the Woodrow Wilson School of Public and International Affairs) from 1977-1980, and in 1979 was a visiting professor at the University of Chicago (Economics).

Prof. Goodman is Contributing Editor for International Perspectives for the ***Communications*** of the Association for Computing Machinery, the world's oldest and largest professional society for computing, and has served with many government, academic, professional society, and industry advisory and study groups. Recently he served as a recognized advisor to the President's Commission on Critical Infrastructure Protection (PCCIP) and organized a series of workshops to assist the Commission, and served as chair of a National Research Council workshop on Technical Responses to Cyber-attack and their Legal Implications. He served as a member of the Defense Science Board Task Force that recommended, among other things, that the ARPANET go public which led to the establishment of today's Internet.

Dr. Goodman has testified before Congress. His research pursuits have taken him to all seven continents and 80 countries, and he has provided Parliamentary or Ministerial-level briefings in many countries including Cuba, Egypt, Israel, Nepal, the Soviet Union, Venezuela, Vietnam, and Zambia, among others.

Prof. Goodman was an undergraduate at Columbia University, where he started out as an English major, and obtained his Ph.D. from the California Institute of Technology (1970), where he worked on problems of mathematical physics.

Brenton C. Greene is the 10th Deputy Manager of the National Communications System (NCS) and is responsible for the day-to-day policy, technical, and programmatic oversight in coordination of all Federal government-wide activities in national security and emergency preparedness communications. He became the Deputy Manager in April 2001.

Prior to his NCS assignment, Greene managed Critical Infrastructure Protection Programs for Sandia National Laboratories, integrating Sandia's significant analytical, research and development, and assessment competencies into national critical infrastructure protection (CIP) initiatives. He was a member of the Defense Science Board 2000 Task Force on Defensive Information Operations.

In 1998-1999, Greene served as Vice President for Electronic Commerce at CAMP, Inc., a non-profit corporation advancing electronic commerce for the Defense Department (DoD) and small and medium size manufacturing enterprises. He managed five Electronic Commerce Resource Centers as part of DoD's National ECRC program.

During 1996 and 1997, Greene was a Commissioner on the President's Commission on Critical Infrastructure Protection (PCCIP), developing national policy and strategy recommendations for the President and leading to a wide range of national CIP initiatives. He was instrumental in the Commission's establishment and its results, and for this, was awarded the Secretary of Defense Medal for Outstanding Public Service.

From 1992 through 1996, Greene was a DoD leader in exploring national security issues pertaining to critical infrastructures and information networks. He created DoD's Infrastructure Policy Directorate, was its first Director for the Under Secretary of Defense for Policy, and was charged with developing policy, plans, programs, guidance and oversight for infrastructure assurance, information and infrastructure warfare concepts.

Mr. Greene served in other key Defense Department positions within the offices of the Under Secretary of Defense (Policy), the Under Secretary of Defense (Acquisition & Technology), the Director, Program Analysis and Evaluation, and the Chief of Naval Operations. In these roles, he coordinated and managed leading edge technology and affordability issues pertaining to information operations, nodal analysis, modeling and simulation, counter-terrorism, satellite capabilities, system security issues, and a broad range of special program technology areas.

A 1971 graduate of the U.S. Naval Academy, Greene completed nuclear propulsion training and served a career in submarines, including tours as commanding officer of the nuclear attack submarines USS Skipjack and USS Hyman G. Rickover. He retired as a Navy Captain in 1995 to continue infrastructure-related initiatives within Government. His military awards include the Defense Superior Service Medal, the Legion of Merit, the Defense Meritorious Service Medal,

the Meritorious Service Medal (two awards), the Navy Commendation Medal (three awards), and the Navy Achievement Medal, as well as various campaign and service awards.

Shannon L. Kellogg is Vice President for Information Security Policy and Programs at the Information Technology Association of America. ITAA, America's leading high tech trade association, provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 400 corporate members throughout the U.S. and Mr. Kellogg manages the industry's largest information security program, with over 175 companies involved in ITAA's Information Security Committee.

Mr. Kellogg leads the Association's national awareness and advocacy efforts on information security and critical infrastructure protection issues. He has served as a coordinator for the IT industry in the development of the President's *National Strategy to Secure Cyberspace*, and served as co-chair of the Partnership for Critical Infrastructure Security Public Policy Working Group in 2001. He is currently a member of Virginia's Commonwealth Information Security Center Advisory Board. Serving as an IT industry spokesperson on information security issues, he has been quoted in numerous national and technology publications, including*: The Wall Street Journal*, *The L.A. Times, The Washington Post, U.S. National Journal's Tech Daily*, and *Federal Computer Week*.

In 2002, Mr. Kellogg developed and implemented ITAA's strategy for a number of legislative successes for the IT Industry on information security, including The Cyber Security Research and Development Act. Mr. Kellogg also led ITAA's successful lobbying efforts to incorporate several key provisions in the Homeland Security Act of 2002 and E-Government Act of 2002, including: removal of legal barriers to critical infrastructure threat information sharing between industry and government, inclusion of the Federal Information Security and Management Act, which will strengthen information security in the federal government, and the Cyber Security Enhancement Act, which strengthens penalties for criminal activity conducted over computer networks.

Prior to becoming ITAA's VP for InfoSec Programs and Policy, Mr. Kellogg served as Executive Director of the Global Internet Project, an international coalition of senior executives committed to fostering continued growth of the Internet. During his tenure at the GIP, he developed a series of projects focused on Next Generation Internet policy issues and chaired the program committee for "Security, Privacy, and Reliability of the Next Generation Internet," a public-private sector dialogue held in Berlin in November 2000.

Mr. Kellogg also has extensive experience in the foreign affairs arena -- with particular regional expertise on Middle East and Turkish affairs – having served as a Program Officer for the International Republican Institute during the 1990s. He also served on President Bush's IT National Steering Committee during the 2000 U.S. Presidential Campaign, and served as a Committee Member of the Arlington Country Republican party in 2000.

Mr. Kellogg received his M.A. in International Business Transactions from George Mason University in Fairfax, Virginia and B.A. in Journalism from Park University in Kansas City, Missouri.

Phillip E. Lacombe is President of the Security Solutions Sector within Veridian, and a corporate Senior Vice President. The Security Solutions Sector of Veridian provides a full range of security services, technology, and expertise to a range of government agencies, principally in law enforcement, intelligence, and defense. Among the sector's offerings are a full suite of information and infrastructure protection services to Federal, State, and Local agencies including: security policy, administration and management, accreditation and certification, counter-intelligence support, counter-terrorism support, analysis, network protection services, forensics and computer emergency response capabilities, and more.

Mr. Lacombe serves on the boards of several organizations including the IT-ISAC, where he is the Vice President of the Homeland Security Institute. He is also a member of several advisory groups for government and private sector organizations.

With Veridian since February 1998, he has served as the corporation's Vice President for Policy and Communications, Senior Vice President for Cyber-Assurance, President of the Information and Infrastructure Protection Sector, and Senior Vice President for Strategic Initiatives before being named President of the Security Solutions Sector in September 2002.

Before joining Veridian, Mr. Lacombe was the Director of the President's Commission on Critical Infrastructure Protection (PCCIP), a position he held from September 1996 until delivery of the Commission's report in September 1997. Established by Executive Order of the President, the PCCIP presented a strategy for dealing with the emerging dimension of cyber threats to the nation's critical infrastructure. With delivery of the Commission report, Mr. Lacombe was named Director of the CIP Transition Office under the National Security Council to support the inter-agency effort that drafted Presidential Decision Directive 63.

Before joining the Commission, Mr. Lacombe was the Managing Director of the Aerospace Education Foundation, a not-for-profit institution providing educational programs nationwide. He also served as the Special Assistant to the Chairman of the Commission on Roles and Missions of the Armed Forces from July 94 through August 95. He was responsible for drafting the Commission's report, "Directions for Defense".

In January 1994, Mr. Lacombe retired with twenty years service as a colonel in the US Air Force. His assignments in the Air Force included Speech Writer to Secretary of Defense Weinberger, Assistant to the Commander of Air Force Systems Command, Counter Narcotics Strategy at the National Drug Policy Board in the Office of the U.S. Attorney General, where he drafted the first national counter-narcotics strategy, and Director of Public Affairs for US and Air Force Space Commands and the North American Aerospace Defense Command.

He is a graduate of the National War College, Air Command and Staff College and Squadron Officers School. He has a Master's Degree from the University of North Carolina and a BA from the University of Massachusetts.

Carl Landwehr, Ph.D., joined the National Science Foundation in October 2001, as Program Director for the newly established Trusted Computing program. He is an IPA from Mitretek Systems, where he is the Senior Fellow in the Center for Information Technology and Telecommunications. In his first two years at Mitretek, he led efforts to support several DARPA activities concerned with Information Assurance and Survivability. Prior to joining Mitretek, he headed the Computer Security Section of the Center for High Assurance Computer Systems at

the Naval Research Laboratory for many years, where he led a variety of research projects to advance technologies of computer security and high-assurance systems. He has also served on the computer science faculty at Purdue University, and he has taught courses on topics in computer science and information security at Georgetown, the University of Maryland, and Virginia Tech. He received a Bachelor of Science degree in Engineering and Applied Science from Yale University and M.S. and Ph.D. degrees in Computer and Communication Sciences from the University of Michigan.

Dr. Landwehr is an Associate Editor of the new IEEE Security & Privacy magazine, and he has served on the editorial boards of IEEE Transactions on Software Engineering, the Journal of Computer Security, and the High Integrity Systems Journal. He was the founding chair of IFIP Working Group 11.3 on Database Security, is a member of IFIP Working Group 10.4 on Dependability and Fault Tolerance, and he has chaired the IEEE Technical Committee on Security and Privacy. IFIP has awarded him its Silver Core, and the IEEE Computer Society has awarded him its Golden Core. His current research interests include information security and dependable systems.

John H. Marburger, III, Ph.D., is the President's Science Advisor and Director of the Office of Science and Technology. He is the former Director of the U.S. Department of Energy's Brookhaven National Laboratory and President of Brookhaven Science Associates.

Dr. Marburger is presently on a leave of absence from the State University of New York at Stony Brook where he served as President and Professor from 1980 to 1994 and as a University Professor of Physics and Electrical Engineering from 1994 to 1997.

Dr. Marburger served as the Dean of the College of Letters, Arts, and Sciences at the University of Southern California from 1976 to 1980. He has been a member of numerous professional, civic, and philanthropic organizations including the Universities Research Association, the Advisory Committee to the New York State Senate Committee on Higher Education, and the Board of Directors of the Museums at Stony Brook.

He is a graduate of Princeton University and received a Ph.D. in Applied Physics from Stanford University.

Marisa Reddy, Ph.D., is the chief research psychologist and research coordinator for the U.S. Secret Service National Threat Assessment Center. In this capacity, she directs all Secret Service research on targeted violence and threat assessment, including the current Insider Threat Study, an operational analysis of insiders who pose a threat to information systems in critical infrastructure sectors. Dr. Reddy's research and training activities focus on applying threat assessment principles to better understand and prevent targeted violence against public officials; in schools and the workplace; and against critical infrastructures and information systems.

Dr. Reddy's career has focused on understanding and preventing violent behavior and on the interface of behavioral science and criminal justice. Prior to joining the Secret Service, she was awarded the James Marshall Public Policy Fellowship at the American Psychological Association, where she worked with congressional staff on violence-prevention legislation and authored testimony for congressional hearings. She has also worked at the Federal Judicial Center and as a consultant to the RAND Corporation.

Dr. Reddy conducts extensive training for local, state, and federal law enforcement, for agencies in the U.S. intelligence community, for school and corporate security personnel, and for international audiences as well. She has a master's degree and Ph.D. in social psychology from Princeton University, and a bachelor's degree from Williams College. Dr. Reddy is author of several publications, and serves on the editorial board of the Journal of Threat Assessment.

O. Sami Saydjari is the founder and Chief Executive Officer of the Cyber Defense Agency, where he provides vision, leadership and expertise for building a Research and Consulting concern that creates effective systematic defenses for high-value systems against aggressive cyber-attack. Before founding the Cyber Defense Agency, Mr. Saydjari was a Senior Staff Scientist in SRI International's Computer Science Laboratory, where he was the program leader of the Cyber Defense Research Center (CDRC). While at SRI, Mr. Saydjari led the survivability assessment of the DARPA UltraLog program, whose goal was to improve the survivability of software agent architectures to solve large-scale distributed applications.

Mr. Saydjari has 18 years of experience performing and directing information assurance research, including 13 years at the National Security Agency and 3 years as a DARPA Program Manager of Information Assurance. Prior to SRI, Mr. Saydjari was the Information Assurance Program Manager for DARPA's Information Systems Office. He created and drove the security architecture and technology for a common reference architecture for DARPA and DISA's advanced programs. His focus areas include high-assurance operating systems, network security, public-key infrastructures, and security architectures. Before his assignment at DARPA, Mr. Saydjari was the technical director of the Office of Network Security Infrastructure for the National Security Agency. In this role, Mr. Saydjari performed an advanced survivability architecture analysis of the MISSI system, including attack trees and fundamental review of required system architecture properties. At NSA, Mr. Saydjari was also the leader of several information assurance research teams in A1 INFOSEC systems design (LOCK), highly assured distributed operating systems design, and trustworthy network systems design.

Mr. Saydjari earned his M.S. in Computer Science from Purdue University. The Director of NSA named Mr. Saydjari an NSA fellow in 1993 and 1994. He has published more than a dozen technical papers in the field of information security and has presented the results of his research at the National Cryptologic Quarterly, the National Computer Security Conference, IEEE Security and Privacy Conference, and the ACM New Security Paradigms Workshop. He is based in Wisconsin Rapids, Wisconsin.

Stephen L. Squires, Ph.D., is vice president and chief science officer for Hewlett-Packard Company. He is responsible for providing leadership in establishing overall strategic, scientific, and technical directions, including the architecture of the digital renaissance for the 21st century Internet.

Prior to joining HP in November 2000, Dr. Squires was the special assistant for Information Technology to the director of the Defense Advanced Research Projects Agency (DARPA). During his career at DARPA, he was responsible for advancing the frontier of progressively larger sectors of information technology. He developed plans for, managed, and directed the scalable systems parts of the DARPA Strategic Computing Program, the Federal High Performance Computing and Communications Program and its extension to the National Information Infrastructure. These programs are recognized as having helped enable the modern

Internet, including its scalable parallel and distributed high-performance computing systems and the introduction of an explicit service layer. He joined DARPA in 1983 as a program manager.

Dr. Squires was recruited by the National Security Agency (NSA) as a freshman undergraduate electrical engineering student at Drexel University. He worked as an engineering intern in the advanced computing and communications laboratories of the NSA. Throughout his career as an electrical engineer and computer scientist at NSA, he focused on the most challenging national security problems using advanced information technologies. In addition, he had early access at NSA to the full range of advanced technologies as they emerged, including many in cooperation with DARPA, such as early interactive time sharing systems with graphics, UNIX, ARPAnet, extensible programming systems, local area networks, the early Internet, personal computing, VLSI design, rapid prototyping and the highest performance information system technologies.

Dr. Squires earned his Ph.D. from Harvard University. He grew up in suburban Philadelphia where he spent most of his time discovering how things worked and inventing in his parents' garage and his own basement laboratory complete with a vacuum tube voltmeter, signal generators, an oscilloscope and a collection of transistors. He also had access to the laboratories of the Franklin Institute Science Museum, local universities, and industry as vice president of his high school's Future Scientists of America program.

Michael Vatis is Director of the Institute for Security Technology Studies (ISTS) at Dartmouth College and the Chairman of the Institute for Information Infrastructure Protection (I3P). ISTS is a principal national center for research, development and analysis of counterterrorism and cybersecurity technology. I3P is a consortium of major research organizations, whose mission is to develop a national R&D agenda for information infrastructure protection, promote collaboration among researchers, and facilitate and fund research in areas of national priority. Mr. Vatis is also Of Counsel with the international law firm of Fried, Frank, Harris, Shriver and Jacobson, specializing in e-commerce and Internet law issues.

Before ISTS, Mr. Vatis founded and served as the first Director of the National Infrastructure Protection Center (NIPC) in Washington, D.C. Now part of the Department of Homeland Security, NIPC was the lead federal agency responsible for detecting, warning of, and responding to cyber attacks, including computer crime, cyberterrorism, and cyber espionage.

Mr. Vatis has also served in the U.S. Departments of Justice and Defense. As Associate Deputy Attorney General and Deputy Director of the Executive Office for National Security, he coordinated the Justice Department's national security activities and advised the Attorney General and Deputy Attorney General on issues such as counterterrorism, high-tech crime, encryption, counter-intelligence, foreign policy, national defense and infrastructure protection. At the Defense Department, Mr. Vatis served as Special Counsel in the Office of General Counsel, advising the Secretary of Defense, the Deputy Secretary of Defense, and the General Counsel on sensitive legal and policy issues.

Mr. Vatis also practiced law with the firm of Mayer, Brown & Platt in Washington, D.C., specializing in Supreme Court and appellate litigation. Before that, Mr. Vatis served as a law clerk for U.S. Supreme Court Justice Thurgood Marshall and for then-Judge Ruth Bader Ginsburg when she served on the U.S. Court of Appeals for the District of Columbia Circuit.

Mr. Vatis earned his law degree from Harvard Law School in 1988 and served as Supervising Editor of The Harvard Law Review. He received his undergraduate degree from Princeton University, where he majored in the Woodrow Wilson School of Public and International Affairs.

APPENDIX G: OFFER FOR OPEN SUBMISSION

APPENDIX G. OFFER FOR OPEN SUBMISSION

A traditional call for papers was not conducted for the 2003 NSTAC R&D Exchange. Instead, participants were given the option to voluntarily submit papers related to the trustworthiness of telecommunications and Information Systems topic. Several participants have submitted papers for the exchange while others may do so in the future. Please go to http://www.ncs.gov/nstac/call_for_papers.html to view the submitted documents.