RESEARCH AND DEVELOPMENT EXCHANGE PROCEEDINGS:

TRANSPARENT SECURITY IN A CONVERGED AND DISTRIBUTED NETWORK ENVIRONMENT

A Symposium Sponsored by the President's NSTAC in Conjunction with the Telecommunications and Information Security Workshop

University of Tulsa

Tulsa, Oklahoma
September 28-29, 2000

MEMORANDUM FOR INDUSTRY EXECUTIVE SUBCOMMITTEE

SUBJECT: 2000 NSTAC Research and Development Exchange Proceedings

On September 28-29, 2000, the President's National Security Telecommunications Advisory Committee (NSTAC), co-sponsored with the Office of Science and Technology Policy (OSTP), held its fourth Research and Development Exchange, in conjunction with the Telecommunications and Information Security Workshop at the University of Tulsa. The purpose of the Exchange was to stimulate an exchange of ideas among representatives from industry, Government and academia on the challenges faced by the convergence of the traditional public switched network (PSN) and the Internet into a Next Generation Network (NGN). During the dynamic dialogues, participants expressed a number of concerns to include: the shortage of qualified information technology professionals, increased litigation, new types of threats, increased vulnerabilities arising from convergence and the need to enhance R&D efforts.

The NSTAC celebrates the continuous efforts of the Research and Development Exchange. 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.

Respectfully,

Henry M. Kluepfel, CPP
Chair, Research and
Development Exchange Task Force

ACKNOWLEDGEMENTS

The President's National Security Telecommunications Advisory Committee (NSTAC) thanks the representatives from industry, government, and academia who participated in the fourth Research and Development (R&D) Exchange held in conjunction with the Telecommunications and Information Security Workshop at the University of Tulsa on September 27-28, 2000. NSTAC would especially like to acknowledge the important contributions of the White House Office of Science and Technology Policy, the Office of the Manager, National Communications System, the U.S. Department of Commerce, and the University of Tulsa for the planning of the 2000 NSTAC R&D Exchange.

Special thanks to the TISW 2000 Chairs, Dr. Don Marks, National Institute of Standards and Technology, Dr. Paul J. Brusil, Telecom Security Institute, Mr. W. Donald Wynegar, National Telecommunications and Information Administration (NTIA), and Dr. Sujeet Shenoi, University of Tulsa. In addition, special thanks to the TISW2000 Program Chairs, Ms. Helen Shaw, NTIA, Mr. James Brenton, Sprint, Mr. Ken Davis, Williams Communications, Mr. Wayne Jansen, Guest Researcher from Switzerland and Mr. John Kimmins, Telcordia Technologies.

TABLE OF CONTENTS

Page Number

EXECUTIVE SUMMARY

Rapid advances in networking technology coupled with the proliferating number of network providers, vendors, and users are raising new security issues and increasing the importance of researching, developing, and deploying new security technology and applications to protect the Next Generation Network (NGN). These changes, compounded by the growth and social acceptance of the Internet, are acting as catalysts for the convergence of the traditional Public Switched Network (PSN) and its Advanced Intelligent Network (AIN) with both public and private Internet Protocol (IP) Networks including the Internet into the NGN. The NGN is a valuable national resource supporting National Security and Emergency Preparedness today and for many years to come. It empowers individuals to transact business online in new ways while allowing total interoperability with traditional communications network services such as E911, and enhances our national security posture. As converged networks offer providers and customers new applications and services, it is important to understand the emerging complex problems affecting the security of the NGN's subcomponents and developing new security technologies, solutions, and applications that will protect those vital resources.

The National Security Telecommunications Advisory Committee (NSTAC) is an advisory committee established in 1982 to provide the President with industry advice on national security and emergency preparedness telecommunications issues. On September 28-29, 2000, the President's NSTAC sponsored its fourth Research and Development (R&D) Exchange. The event was conducted in conjunction with the Telecommunications and Information Security Workshop 2000 (TISW2000) held at the University of Tulsa in Tulsa, Oklahoma on September 27-28, 2000. The purpose was to stimulate an exchange of ideas among representatives from industry, Government, and academia on the challenges posed by network convergence. Discussions of convergence issues as TISW2000 and the R&D Exchange led to the following conclusions:

- The shortage of qualified information technology (IT) professionals, particularly those with expertise in information assurance and/or computer security, remains a major impediment to strengthening the security of the NGN. The participants believed programs, such as the Scholarship for Service program under the Federal Cyber Service Initiative and others designed to create financial incentives for students to pursue computer security disciplines at the graduate and undergraduate levels, need to be implemented.

- The Information Assurance (IA) Centers of Excellence program, sponsored by the National Security Agency (NSA), is an excellent initiative to recognize and help address the growing demand for computer security professionals but needs to be expanded beyond the current 14 schools. Moreover, a need exists to make information about the IA Centers of Excellence and other information assurance and security curricula and certifications available to other schools, such as community colleges and technology trade schools. In addition, participants encouraged cyber ethics training at the K-12 level.

- The Partnership for Critical Infrastructure Security represents an important step in enhancing the relationship between the private sector and the Government, but wider participation by academia and officials in State and local governments is needed.

-
- Developing a business case for security poses difficult challenges in the commercial sector, and there is a need to offset the high costs and high risks associated with R&D in security technology. Tax credits and other financial incentives might allow companies to minimize their risks and encourage commercial enterprises to increase the funding of security technology R&D.

- Given the complexity and interdependence introduced to networks by convergence and the proliferation of network providers and vendors, best practices, standards, and protection profiles that help to ensure secure interoperable solutions must be evenly applied across the NGN.

- There is a need to enhance R&D efforts to develop better testing and evaluation programs to reduce the vulnerabilities introduced by malicious software. While securing the transmission of voice and data remains an important concern, it is equally important to identify emerging security vulnerabilities in the network control space.

- New types of threats, such as distributed denial of service attacks, challenge corporations to develop security policies and procedures to protect themselves from liability claims. For example, new legal precedents, case law, and Federal legislation such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Financial Modernization Act of 1999 are creating a HIPPA like standard of due care forcing organizations to take new security measures to protect against anticipated threats or hazards to the security or integrity of customer records and information or risk civil litigation.

- Although technology remains an important component in building security solutions, it is vital to conduct research activities in other areas such as operations, legal and public policy, and human factors. The efficacy of technological solutions is often dependent on the ability of human operators to properly implement, administer, and manage the technology consistent with company policy and the legal constraints.

- There is a continuing need to sponsor joint events like TISW2000 and the R&D Exchange that facilitate a dialogue among representatives from industry, Government, and academia. All three communities play a crucial role in the R&D of security technologies and applications, and participants described how holding events at universities with IA programs offered unique benefits. Most notably, such events allow security practitioners from industry, Government, and academia to share views and opinions on R&D issues, solutions and challenges in an informal, research-oriented setting.

The participants at the R&D Exchange offered several recommendations for consideration by the Government and NSTAC. The thrust of these recommendations is to improve the security of

networks in a converged and distributed environment.

The Government should:

- Establish and continue to fund Government programs to encourage increasing the number of graduate and undergraduate students pursuing study in computer security disciplines. Those programs include national initiatives such as the Scholarship for Service program under the Federal Cyber Service initiative to ensure that the Government educates, trains, and retains access to highly qualified IT security professionals.

- Increase the funding and support to the National Security Agency and other Government agencies to facilitate the certification of additional IA Centers of Excellence to train and educate the next generation of information technology security professionals.

- Develop tax credits and other financial incentives to encourage industry to invest more capital in the research and development of security technologies.

- Expand partnerships on critical infrastructure protection issues by encouraging more representatives from academia and State and local governments to participate.

- Invest in R&D programs that encourage the development of best practices in NGN security, such as improved testing and evaluation, broadband protection profiles, and NGN security standards.

To support the Government, the NSTAC should:

- Consider the issues of best practices and standards its report to NSTAC XXIV.

- Consider the evolving standards of due care legal issues discussed at the R&D Exchange, including linked or third party liability and new privacy legislation and regulations such as HIPAA.

- Conduct another R&D Exchange in the Fall of 2001 in partnership with one or more of the IA Centers of Excellence to continue the dialogue with Government and academia. The purpose of that exchange should be to discuss the difficulties in and strategies for both increasing the number of qualified IT security professionals and enhancing the academic curricula to meet the security challenges of the NGN.

RESEARCH AND DEVELOPMENT EXCHANGE

Transparent Security in a Converged and Distributed Network Environment: A Dream or a Nightmare?

Proceedings

1.0 INTRODUCTION

The National Security Telecommunications Advisory Committee (NSTAC) is a Presidential advisory committee established in 1982 to provide the President with industry advice on national security and emergency preparedness (NS/EP) telecommunications issues. On September 28-29, 2000, the President's NSTAC sponsored its fourth Research and Development (R&D) Exchange. The event was conducted in conjunction with the Telecommunications and Information Security Workshop (TISW) 2000 held at the University of Tulsa in Tulsa, Oklahoma. The purpose was to stimulate an exchange of ideas among representatives from industry, Government, and academia on the challenges posed by the convergence of the traditional public switched network (PSN) and the Internet into a Next Generation Network (NGN).[1[1]] While the NGN might not be fully realized for several years, the impact of convergence of the control space of the PSN with that of the Internet is of increasing concern today. It is that concern that prompted the sponsoring of TISW 2000 and the R&D Exchange.

This document presents an overview of the TISW 2000 and the R&D Exchange. Section 2.0 summarizes the keynote presentation, panel sessions, and facilitated discussions at the R&D Exchange. Section 3.0 captures observations distilled from the three tracks of the TISW 2000: Telecommunications Security, Critical Infrastructure Protection, and the R&D Exchange. Section 4.0 highlights the conclusions and recommendations developed by the participants at the R&D Exchange designed to improve the Nation's efforts to prioritize its R&D investments and focus on the unique security challenges posed by network convergence.

1.1 Background

Rapid advances in networking technology coupled with the proliferating number of vendors, network providers, and users are raising new security issues and increasing the importance of researching, developing, and deploying new security technology and applications to protect the NGN. These changes, compounded by the growth and social acceptance of the Internet, are acting as catalysts for the convergence of the PSN and Internet Protocol (IP) Networks into the NGN. The NGN is a valuable national resource. It empowers individuals to transact business

[1[1]] The Information Technology Progress Impact Task Force to NSTAC XXIII in June 1999 states that the "Next Generation Network is a public, broadband, diverse, and scalable packet-based network evolving from the public switched network, advanced intelligent network (AIN), and the Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence. That same report states that "convergence indicates a process over a 3- to 5-year period of NGN evolution during which traditional circuit-switched networks (including AIN) and IP-based networks will coexist and interoperate to enable end-to-end transmission of voice communications, until IP-based networks subsume circuit-switched networks.

online in new and innovative ways; provides a continuing source of economic vitality and growth; promotes national competitiveness and productivity; and enhances our national security posture. As converged networks offer providers and customers new applications and services, it is important to develop new security technologies, solutions, and applications that will protect that vital resource.

The fourth R&D Exchange results from a continual effort by the NSTAC to examine the risks to the security of the PSN. In examining these risks, the NSTAC grouped its efforts into four interrelated categories: embedded interoperable security, network security, critical infrastructure protection, and network convergence. The following paragraphs elaborate on these concepts.

1.1.1 Embedded Interoperable Security

At the NSTAC XXII meeting held on June 9, 1999, the Honorable John Hamre, Deputy Secretary of Defense, discussed the need for open dialogue between industry and Government in the current era of dynamic technological change. Dr. Hamre requested NSTAC's assistance to, "tackle the much deeper, more complicated problem, which is how do we embed security in depth in the infrastructure upon which we, the Government, depend, and upon which you and your customers depend." The NSTAC's Industry Executive Subcommittee (IES) subsequently began to examine this issue to determine how to respond to Dr. Hamre's request.

The Embedded Interoperable Security Scoping Group was established to explore the issue and received briefings from the National Security Agency (NSA), the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, the General Services Administration, and the Defense Information Systems Agency. The group concluded that there was no clear role for NSTAC, which was created to provide the President with policy advice, in addressing the challenges associated with embedding interoperable security into the information infrastructure. However, it was agreed that NSTAC could address the technical challenges and highlight best practices related to embedded interoperable security solutions in its next R&D Exchange.

1.1.2 Network Security

In response to the growing prevalence of hacker incidents and other forms of electronic attacks, the NSTAC formed the Network Security Task Force (NSTF) in 1990 to assess the threats to and vulnerabilities of the PSN. The task force identified six areas in which R&D on commercially applicable security tools was needed:

- A mechanism for easy, portable control of access to a network element, ideally uniform across the industry
- A development to introduce an appropriate level of "suspicion" among trusted elements of the PSN
- Solutions for reliable recovery from damage to software and databases

- Means to adequately partition memory, or otherwise isolate network element software from databases that are more broadly accessed

- Means to analyze all events in a network and highlight questionable situations

- Tools to plan an architecture toward a long-term, more secure network.

In 1991, the Government and NSTAC Network Security Information Exchanges (NSIE) were formed to facilitate regular meetings of network security practitioners from industry and Government with the purpose of exchanging information on network vulnerabilities, computer intrusions, and other events. The Government and NSTAC NSIEs continue to meet regularly and they periodically publish an assessment of the risks to the security of the PSN. The most recent version of that risk assessment, entitled *An Assessment of the Risk to the Security of the Public Network,* was published in 1999.[2[2]]

As part of its ongoing network security activities, the NSTAC periodically sponsors R&D Exchanges to stimulate a dialogue among industry, Government, and academia. Since 1991, the NSTAC has sponsored three R&D Exchanges:

- **First R&D Exchange (1991)**
  The first R&D Exchange was actually two separate events in 1991 intended to provide a forum for industry and Government officials to discuss the six technology areas listed above and to exchange information about ongoing R&D projects. In the first session, officials from the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) presented their views on security technology R&D issues. In the second session, representatives from industry provided their perspectives on researching and developing security technologies.

- **Second R&D Exchange (1996)**
  The second R&D Exchange was conducted in September 1996 to facilitate a common understanding of network security problems affecting NS/EP telecommunications, to identify R&D programs in progress to address those problems, and to identify future security technology R&D needs. Four broad security topics were discussed: authentication, intrusion detection, integrity, and access control.

- **Third R&D Exchange (1998)**
  The third R&D Exchange was sponsored in conjunction with the White House Office of Science and Technology Policy (OSTP) and Purdue University in October 1998 to examine collaborative approaches to security technology R&D. The participants also discussed the need for training more information technology security professionals, creating large-scale test beds to test security products and solutions, and promoting the creation of Information Assurance (IA) Centers of Excellence in academia.

[2[2]] Copies of the NSIE Risk Assessments are available upon request from the Office of the Manager, National Communications System (www.ncs.gov).

One of the major findings and recommendations from the 1998 R&D Exchange was for the NSTAC to sponsor a fourth R&D Exchange in 2000 that included participation from industry, Government, and academia and focused on topics related to network convergence.

1.1.3 Critical Infrastructure Protection

Beginning in 1995, concerns about the potential threat of an information warfare attack against the United States and its critical infrastructures attracted the attention of senior Government and industry officials. For the past five years, NSTAC has worked closely with the U.S. Government on critical infrastructure protection issues. Specifically, at the request of the President, NSTAC examined the information-based risks posed to the electric power, financial services, and transportation infrastructures[3[3]] and coordinated its activities with the President's Commission on Critical Infrastructure Protection. In 1997, the NSTAC studied the state-of-the-art in intrusion detection technology and assessed the role that technology might play in protecting critical telecommunications and information systems.

On May 22, 1998, President Clinton signed Presidential Decision Directive 63, *Critical Infrastructure Protection,* which outlined a national critical infrastructure protection strategy with the intent of eliminating or otherwise mitigating significant vulnerabilities in critical infrastructures. Improved technologies through national R&D programs were identified as a key element of this strategy. Building on that directive, the White House released *The National Plan for Information Systems Protection: An Invitation to a Dialogue* (Version 1.0) in January 2000 that identified enhanced security technology R&D as one of the Administration's 10 CIP programs. Specifically, that plan called for increased R&D in the areas of prevention, intrusion detection, and recovery technologies.

More recently, NSTAC formed the Information Sharing and Critical Infrastructure Protection Task Force following NSTAC XXII to serve as the focal point for addressing critical infrastructure protection issues. The task force is currently focusing on developing and coordinating NSTAC input to *National Plan for Information Systems Protection, Version 2.0,* which addresses efforts to prioritize and maximize the return on the Nation's R&D investment.

1.1.4 Network Convergence

In June 1999, the NSTAC formed the Information Technology Progress Impact Task Force to address how the progress of information technology, namely the convergence of the evolving intelligent PSN and IP networks, might affect NS/EP priority telecommunications services. The task force concluded that as the converged NGN public network evolves, telecommunications carriers' Signaling System 7 (SS7) networks would become less discrete and more reliant on IP technology and interfaces. Therefore, the task force concluded that the security, reliability, and availability of the NGN control space as they relate to the provision and maintenance of NS/EP services capabilities needs to be considered. Furthermore, in examining evolving network technologies that could support NS/EP requirements in both converged networks and the NGN, the task force concluded that quality of service and other NGN capabilities would likely require enhancements to best satisfy specific NS/EP requirements.

[3[3]] Letter from the President of the United States to Mr. William Esrey, NSTAC Chair, dated July 7, 1995.

Consequently, the task force recommended that the President direct the appropriate Federal departments and agencies, in coordination with industry, to determine precise functional NS/EP requirements for converged networks and the NGN, and ensure that such requirements are conveyed to standards bodies and service providers during NGN standards development and implementation. Following the issuance of the task force's report, the NSTAC established the Convergence Task Force (CTF) and tasked it to examine the potential NS/EP implications of potential security and reliability vulnerabilities of the control space in the NGN.

1.2 R&D Exchange Objectives

The primary objectives of the R&D Exchange were to facilitate a dialogue among industry, Government, and academia and discuss emerging security issues associated with network convergence. To stimulate robust discussions on this topic, panelists and participants were selected to present the views of vendors, network providers, users, and regulators.

2.0 R&D EXCHANGE OVERVIEW

This section summarizes the keynote presentation, panel sessions, and facilitated discussions at the R&D Exchange. On September 28-29, more than 100 representatives from industry, Government, and academia participated in NSTAC's fourth R&D Exchange. The theme for the 2-day event was "Transparent Security in a Converged and Distributed Network Environment: A Dream or a Nightmare?" This section details the activities of the R&D Exchange.

2.1 Keynote Presentation

The first day began with a keynote presentation by Representative Curt Weldon (R-PA), who discussed the importance of protecting our Nation's telecommunications and information systems from an array of new threats. Congressman Weldon described his role as a leader on the National Defense Committee in the U.S. House of Representatives. He described a two-pronged challenge facing the Nation. First, he emphasized the importance of maintaining information dominance on the battlefield. Second, he pointed to the growing threat posed by cyber terrorism. To address those challenges, Congressman Weldon identified three broad recommendations. The first was to develop technical tools and capabilities to collect, aggregate, mine, and share threat information. The second was to invest in R&D programs to ensure that the U.S. military retains access to cutting-edge information technologies on the battlefield. The third was to train the next generation of computer security professionals. Following his keynote remarks, Congressman Weldon participated in an interactive question and answer period.

2.2 Panel on Differing Perspectives on Security in Converged Networks

The keynote presentation was followed by a panel discussion moderated by Dr. Peter Fonash, Chief, Technology and Programs, National Communications System (NCS). The panel focused on offering differing perspectives on security in converged networks. Dr. Fonash opened the panel discussion by providing an overview of convergence issues, describing the technology programs at the NCS, and introducing the panelists.

Dr. Paul Prucnal, Princeton University, presented a tutorial on optical networking technologies and their potential for impacting the Next Generation Internet and the NGN. He highlighted the high demand for bandwidth, and noted the reason most often cited for shortfalls was the limited capacity of fiber optic cable to transmit high-speed data. He commented, however, there was a great deal of unused bandwidth on fiber optic cables and that the bottleneck was really the inability of routers to manage the flow of data. He emphasized that advanced research in the area of optical routing and switching may enable increased bandwidth availability in the future. Mr. Robert Wright, BellSouth, provided a network provider's perspective on managing risks, described the dilemma experienced by many corporations in balancing the need for security versus the benefits of utility and accessibility, and outlined several mitigation strategies. Mr. Edward Balkovich, Verizon, focused on security issues related to integrated voice and data networks and Voice over IP technology. He also emphasized the importance of focusing on the SS7 to IP security interconnections, where attacks are most likely to occur.

Mr. Dan Woolley, Global Integrity, provided an overview of the increased incidence of electronic intrusions and described the costs associated with security incidents and recovery operations. Dr. Jack Edwards, Nortel Networks, emphasized the importance of considering security in the control space, noting that it is a shared responsibility. He also described the importance of devoting R&D to developing better test and evaluation methodologies to identify malicious code in software programs.

2.3 Panel on Technology Transfer Issues

The second day of the R&D Exchange opened with a panel discussion on Technology Transfer Issues moderated by Mr. Hank Kluepfel, SAIC. Dr. Gif Monger, SAIC, described the netEraser program that was partially funded by In-Q-Tel, whose mission is to fill critical R&D gaps by funding emerging and/or high-risk technologies. The netEraser program was established to provide secure network services across the highly vulnerable environment of today's Internet and, in essence, create a secure – or ".scom" – domain. The purpose of netEraser is to create a robust secure gateway for electronic commerce and other transactions that is less transparent and vulnerable to hacker attacks. Mr. Paul Krumviede, WorldCom, highlighted several areas where government and industry have collaborated or traded technologies, particularly with respect to the Internet, and identified several key challenges to the effective transfer of technologies.

2.4 Recap of Events and Facilitated Discussion

Following the last panel discussion, Mr. Kluepfel, Dr. John Hale, University of Tulsa, and Dr. Terry Kelly, Office of Science and Technology Policy, summarized the main issues of TISW 2000 and the R&D Exchange. Following that summary, the R&D Exchange concluded with a facilitated discussion that identified key issues and challenges associated with security in converged networks. Figure 1 lists observations derived from the facilitated discussion.

The R&D Exchange Agenda and List of Attendees are attached in Appendix A.

Figure 1. Discussion Topics from the Facilitated Session

Discussion Topics	Key Points
Shortage of Information Technology Security Professionals	• Advocate funding of Scholarship for Service program • Develop cyber ethics training and educational programs at the K-12 level to complement the Scholarship for Service program • Maintain and increase number of professors, possibly by extending the Scholarship for Service program to include incentives for individuals to teach • Create educational programs that are responsive to economic conditions (e.g., fund fellowships/scholarships, endow teaching positions)
Broaden Critical Infrastructure Protection Partnerships	• Continue to sponsor joint industry-Government-academia forums • Conduct more outreach with all communities (e.g., community colleges) • Include broader participation by academia in critical infrastructure security activities (e.g., Partnership for Critical Infrastructure Security, Institute for Information Infrastructure Protection) • Stimulate international cooperation of critical infrastructure protection • Engage State and local governments and regional organizations in critical infrastructure protection activities • Simplify education and awareness programs (e.g., create a parallel program to the McGruff "Take A Bite Out Of Crime" program)
Incentives for Security	• Support tax considerations and incentives to promote security R&D • Extend programs/incentives similar to the In-Q-Tel program • Develop creative funding mechanisms for R&D investment and technology transfer
Best Practices	• Develop broadband protection profiles supported by industry and Government • Train law enforcement on investigations in commercial operating environments • Identify a centralized point for discussing/promulgating standards • Develop testing and evaluation procedures to help identify malicious code
Holistic View of Security Technology R&D	• Address legal/regulatory frameworks related to converged networks • Focus research agenda on topics broader than technology to include operational issues, legal and policy, and human factors • Embrace a broader R&D agenda; focus on analysis (data reduction, forensics) • Adopt both long-term (25 years, basic research) and short-term (3 years, applied development) approaches • Consider the full lifecycle perspective on R&D issues

3.0 WORKSHOP OBSERVATIONS

This section describes the major observations from the three TISW 2000 tracks: the Telecommunications Security track sponsored by NIST; the Critical Infrastructure Protection track sponsored by the National Telecommunications and Information Administration; and the R&D Exchange track sponsored by NSTAC. Those observations were presented and capture on a non-attribution basis.

3.1 The Telecommunications Security Track

The Telecommunications Security track of TISW 2000 focused on the security issues and solutions emerging as information networks are integrated into the existing telecommunications networks to support both telephony and data services. That track consisted of five sessions:

- Security in Convergent Telecommunications and Computer Networks
- Security Vulnerabilities in Emerging Technologies
- Standards for Telecommunications Security
- Security Issues of Network Integration
- Secure Telecommunications Network Management.

During those sessions, three major themes emerged relevant to the discussions in the R&D Exchange. These themes are summarized below.

3.1.1 Security Vulnerabilities of Converged Networks

In the context of the continuing transition to converged networks and the NGN, participants discussed the need to develop comprehensive security architectures commensurate with the evolving network infrastructure and technologies. Although customer requirements remain the primary drivers for security architectures, participants noted that good business practices dictate that security benchmarking and best practices are needed to facilitate the evolution of a secure and reliable NGN. This goal, however, cannot be achieved without a comprehensive understanding of the potential security vulnerabilities of converged networks. Those vulnerabilities include weaknesses introduced through facilitation of control space interactions between the PSN and IP networks (e.g., SS7). Participants noted that converged network control space vulnerabilities could result from the inadequacy and unreliability of existing gateway screening capabilities, the lack of security guidelines for interconnection, and lack of mechanisms to control or authenticate network management traffic and routing on the network. Such vulnerabilities could enable, for instance, the insertion of false SS7 message commands into the PSN via IP networks.

A potential solution discussed at the conference involved adopting “signaling” firewalls for the PSN signaling gateway that serve similar functions to those on the Internet. Such solutions can be analyzed and adopted through a risk management approach in which current security infrastructure and processes are leveraged with new tactical technologies and processes to gain a higher level of security capabilities. Moreover, additional vulnerabilities can be introduced when new technologies are installed; therefore, embedded security capabilities defined through

standards are less precarious. Furthermore, producers of commercial-off-the-shelf security products must be made aware of specific customer security requirements to be able to include sufficient security capabilities. It was noted that in most instances reliance on third-party evaluation might offer an effective means to ensure compliance with security requirements. One cited example was NIAP, which offers product and system security testing and evaluation through common criteria testing labs. This process enables vendors to effectively build and test products against a specific user-defined protection profile.

3.1.2 Standards and Protocols

Conference participants emphasized that adopting standards and protocols in support of network security is essential to advancing the transition to the NGN. For instance, the Internet Engineering Task Force (IETF) proposed draft Stream Control Transmission Protocol (SCTP), which is designed to enable the secure transport of PSN signaling messages over IP networks. The design of SCTP includes congestion avoidance behavior and resistance to flooding and masquerade tactics common in distributed denial of service attacks. IP networks in general will require a broad spectrum of effective security protocols to enable secure transmission of voice and data traffic. For instance, IP Security is a network layer protocol enabling end-to-end cryptographic security services to support the secure exchange of packets. Several protocols are also being developed to support security of voice over the Internet (VOI) such as H.323 and Session Initiation Protocol (SIP). Organizations such as the IETF and the European Telecommunications Standards Institute (ETSI) Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) group are researching these technologies. Industry contribution to standards bodies activities on these evolving protocols is viewed as extremely important because that participation means security mechanisms can be incorporated from inception rather than having to build on existing capabilities. This early involvement is essential because the security "add-on" approach through downloadable software patches can insert additional vulnerabilities by contravening existing security measures.

3.1.3 Managing Security in Converged Networks

A major topic of discussion was the need to build a business case rationalizing executive management commitment for investing in network and information security solutions in the converged network environment. Participants also noted the importance of implementing and enforcing dynamic security procedures; educating and training employees on the organization's security policies, procedures, and practices; and cooperating with law enforcement where appropriate. A significant challenge, however, is to adopt security technologies and policies that are not too inhibitory. The competitive environment in the telecommunications and information technology industries requires balancing the need for a robust security infrastructure that cannot be compromised and ensuring the network is not overtaxed to the extent that network speed and traffic flows are affected. In essence, security should be transparent to users and not unduly affect network performance.

3.2 The Critical Infrastructure Protection Track

The Critical Infrastructure Protection track of TISW 2000 focused on the challenges posed by emerging threats to the Information and Communications (I&C) sector. That track consisted of five sessions, which are listed below:

- CIP Practices and Guidelines for Small and Medium-Sized Businesses
- CEO-Level Concerns for Legal and Business Consequences of InfoSec Threats
- Risk Management Process and Risk Assessment Tools
- The Case for Partnership
- International CIP Policy Perspectives.

During those sessions, three major themes emerged relevant to the discussions in the R&D Exchange. These themes are summarized below.

3.2.1 Legal Issues

Legal issues surrounding the security of the I&C sector arose as a major topic of the Critical Infrastructure Protection track. In describing the business case for security, several speakers related how the legal issues that were increasingly capturing the attention of executives afforded security professionals an opportunity to demonstrate how good security is not a cost center but protects the corporation's interests. Several legal case studies were presented to demonstrate how poor security practices exposed an organization to considerable risk. For example, one topic discussed was the concern over *linked* or *third-party* liability. Those concepts stemmed from the distributed denial of service (DDOS) attacks launched against Yahoo, e-Bay, CNN, and other Internet-based businesses in February 2000. It was noted that the victims of the DDOS attacks could have attempted to pursue civil litigation against the Web sites that were used as the launching point for those attacks. Those sites included several Internet service providers. The issue of linked liability led to a discussion of standards of due care that should be taken by commercial and public entities to ensure that their networks and information systems are safe from, and cannot be used in, third-party attacks. Several speakers emphasized the importance of documenting threats and countermeasures and other actions taken to protect systems as part of a larger due diligence process.

Privacy was another key topic discussed throughout the course of TISW 2000. Several speakers pointed to the growing prevalence of privacy legislation and regulation at all levels of Government. It was noted that recent actions by the Federal Trade Commission to develop and enforce Internet privacy and the protection of customer information guidelines were seen as a watershed event triggering a host of privacy legislation and regulation. With the growing interest in protecting customer information, legislators and regulators were turning to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 as a model for new privacy protections. HIPAA provides for the protection of the integrity and confidentiality of patient medical records. Several presenters noted that the privacy protections and language embedded in the HIPAA legislation and subsequent rules are being applied to other sectors.

For example, participants stated that provisions in the Banking Modernization Act of 1999 (known as Gramm-Leach-Bliley) applied HIPAA-like language to the financial services industry in regulating how it handles and uses customer information. Gramm-Leach-Bliley creates new protections for consumer privacy, specifically ensuring that all customers will know how their confidential information will be treated and shared. Relevant to protection of consumer information, the Securities and Exchange Commission issued regulations that apply to publicly held and traded companies. Another important factor cited at the conference is the growing role of State laws in the area of privacy. It was noted that States were creating new laws to protect the privacy rights of citizens and the result might be 50 different standards and practices for privacy across the United States that companies would need to be cognizant of.

In the final analysis, many participants described how the growing prevalence of new laws, case law, and legal precedents was forcing corporations to reconsider the importance of security and related due diligence processes. The new standards of due care set by legislation such as HIPAA and Gramm-Leach-Bliley are forcing government agencies and commercial enterprises to consider their evolving fiduciary responsibilities and exposure to litigation.

3.2.2 Information Sharing

Information sharing is a key element in the President's national strategy for critical infrastructure protection and was discussed in-depth at TISW 2000. Specifically, participants identified five obstacles to greater sharing of information on electronic intrusions. First, it was noted that the unwanted publicity generated by the revelation of a computer intrusion could harm shareholder interests. Second, there was considerable discussion about the role and practices of law enforcement in investigating computer intrusions. Several participants maintained that there was a need to better train law enforcement officials to ensure that their investigations do not disrupt service or unnecessarily damage equipment. The third obstacle was concern about anti-trust issues, specifically balancing the inclusiveness in sharing information against the fear of anti-trust violations (or even the appearance thereof). Fourth, the provisions of the Freedom of Information Act (FOIA) were addressed from the perspective of how these provisions might influence the willingness of corporations to reveal network vulnerabilities to Government only to have them revealed under a FOIA request. Fifth, corporations were said to be hesitant to share information because of uncertainty about how information would be handled, sanitized, and disseminated by the Government or Information Sharing and Analysis Centers.

3.2.3 The International Nature of CIP

One of the major themes of the conference was how critical infrastructure protection issues had gained international attention. It was noted that foreign governments and corporations are becoming more aware of information security concerns, and that the NGN will be significantly influenced by the global reach of the telecommunications and information technology industries. Several speakers emphasized the need for greater cooperation across international borders with respect to sharing information on cyber threats and cyber crime, investigating and prosecuting computer intruders, and developing better security standards to protect the NGN.

3.3 Research and Development Exchange Track

The R&D Exchange's theme was "Transparent Security in a Converged and Distributed Network Environment: A Dream or a Nightmare?" During that track, five major themes emerged that are summarized below.

3.3.1 Shortage of IT Security Professionals

Participants at the R&D Exchange described the continuing problem of a shortage in qualified IT security professionals measured against the growing demands of Government, industry, and academia. Specifically, it was noted that the Government and academia face considerable recruitment and retention issues when competing with the private sector for the scarce pool of professionals. For example, participants described the difficulty in recruiting and enticing candidates into computer security Ph.D. programs when they can command high salaries in the marketplace. The potential solutions discussed by the participants included:

- Expanding fellowship programs
- Enhancing work-study programs
- Granting leaves of absence to industry experts for a year to teach at a university
- Securing industry grants for endowed teaching positions.

Participants also discussed the need to create and support Federal programs like the Scholarship for Service program, which provides scholarship money for students to pursue undergraduate and graduate education in the area of computer security.[4[4]] It was suggested that efforts to increase the number of undergraduate and graduate students should be complemented by cyber ethics and computer education programs at the K-12 level and extending the Scholarship for Service program to include financial incentives for individuals to pursue teaching. Moreover, there was consensus regarding the need to increase the number of Information Assurance (IA) Centers of Excellence.[5[5]] Currently, fourteen academic institutions are accredited as IA Centers of Excellence, and participants agreed the number needed to increase over the next 5 years.

[4[4]] The Scholarship for Service was program is one of five education and training programs included in the National Plan for Information Systems Protection under the Federal Cyber Service (FCS) initiative. That initiative was funded by the Defense Authorization Act for Fiscal Year 2001. The FCS initiative recognizes that a dearth of educated and trained IT security professionals exist. On October 27, 2000, President Clinton announced a Scholarship for Service program that provides up to two years of scholarship funding for students studying information security in return for a commitment to work for an equal amount of time for the Federal Government. The scholarship program will be administered by the National Science Foundation through grants to selected colleges and universities recognized as having mature information security education programs.

[5[5]] The National Security Agency (NSA) sponsors the Information Assurance Center of Excellence program, which designates universities as centers of academic excellence for training information security professionals. NSA "grants the designations following a rigorous review of university applications against published criteria based on training standards established by the National Security Telecommunications and Information Systems Security Committee. NSA's establishment of this program was spurred by the growing demand for professionals with Information Assurance expertise in various disciplines. The Centers for Academic Excellence may become focal points for recruiting and may create a climate to encourage independent research in Information Assurance."

3.3.2 Broaden CIP Partnerships

Presidential Decision Directive 63 called for the creation of a public-private partnership to protect critical infrastructures. Several participants described efforts over the past 18 months to build an effective partnership between industry and Government. They agreed that the progress thus far was encouraging and emphasized the need to enhance the participation by academia and State and local governments. Specifically, participants stated that the Partnership for Critical Infrastructure Security[6[6]] was a good first step but advocated efforts to increase awareness of its activities in academia and in the State and local government community to encourage broader participation. One area cited where academia could contribute was the proposed Institute for Information Infrastructure Protection (I3P).[7[7]] The goal of that institute is to serve as the focal point for research in the area of IA. Several participants commented that there was a high level of industry representation on the I3P's Board of Directors, but only two of the proposed members represented academia. Given the research focus of the I3P, they suggested increasing involvement by leaders in security research at the Nation's colleges and universities.

3.3.3 Incentives for Security

A major topic at both TISW 2000 and the R&D Exchange was creating incentives for companies and other organizations to invest in security. In particular, many participants cited the difficulties in quantifying the returns on investment as a major impediment to developing strong business cases for security. Three options for creating incentives for security were discussed:

- Alternative and creative ways for Government to fund and encourage R&D were considered and discussed. For example, it was noted how the Central Intelligence Agency played a key role in creating In-Q-Tel, whose mission is to fill critical R&D gaps by funding emerging and/or high-risk technologies. In many cases, those technologies may not have an immediate commercial market. However, they are important to promoting the security of telecommunications and information networks. It was suggested that more programs like In-Q-Tel be created to offer industry more access to capital for investing in innovative security technologies and facilitating the transfer of technology between industry and Government.

- It was also suggested that further examination of legal issues would assist in building a strong business case for security. Participants emphasized the growing importance of liability issues and described how well documented security policies and programs are the best protection against exposure to civil litigation.

[6[6]] For more information on the PCIS, PDD-63 and the other critical infrastructure protection initiatives, please refer to the Critical Infrastructure Assurance Office Web site at http://www.ciao.gov/.

[7[7]] It should be noted that the I3P shares many of the same attributes and objectives of the proposed Information Systems Security Board (ISSB) proposed by NSTAC in 1997. The proposed ISSB was conceptualized as a private sector entity that would promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services.

- Tax credits were suggested as a possible financial incentive for stimulating research in security technologies. It was noted that the type of research being performed by industry, perhaps best described as applied development, was capital intensive and high risk. Industry participants noted that if companies could offset some of those risks through tax credits, overall industry investment in security technology R&D might increase significantly; the result might be a growing willingness in the private sector to take risks in researching emerging technologies.

3.3.4 Best Practices

Throughout the TISW 2000 and R&D Exchange events, the need to develop best practices in the area of telecommunications and information security was consistently voiced. Five different areas involving best practices were discussed over the course of the 3-day event:

- The first is to research and develop better testing methodologies to identify flaws and malicious code in software. It was noted that future testing should go beyond seeking out bad or hidden code to identify malicious code in software programs that might be exploited or activated by potential intruders.

- The second is to develop policies and procedures for continually reviewing and updating software. A common problem affecting network security is that system administrators fail to update their systems with software patches. This oversight leads to conditions that present electronic intruders with opportunities to exploit known vulnerabilities and gain unauthorized access to systems.

- The third is to develop broadband protection profiles that allow vendors and network providers to assess the quality of security solutions in the converged network environment and evaluate those solutions against common scenarios.

- The fourth is to conduct due diligence reviews of company policies and procedures that include business contingency planning and identification of new threats. It was noted that risks should be assessed regularly as new technologies are introduced and integrated into the NGN.

- The fifth is to work with law enforcement to develop better methods for investigating computer intrusions with the goal of ensuring proper procedures/practices without unduly affecting the system's performance.

3.3.5 Holistic View of Security Technology R&D

Another major discussion point of the R&D Exchange was the need to adopt a more holistic and balanced view of security technology R&D in three contexts. First, participants noted that the public and private sectors are undertaking a tremendous amount of research in security technologies. However, R&D investment tends to concentrate on applied development of security technologies and solutions with immediate commercial appeal. Participants described the need to balance this focus on applied development with an increased emphasis on basic

research in new and innovative security technologies. Second, there was agreement that the focus of R&D programs tends to over-emphasize technology and should broaden to include other important aspects of sound security such as operations, legal and policy, and human factors. Third, participants discussed the need to weigh short-term R&D objectives and funding common to Federal procurements/grants and industry funding of universities against the desire of academia to focus on long-term research priorities.

4.0 CONCLUSIONS AND RECOMMENDATIONS

The R&D Exchange once again offered a forum for representatives from industry, Government, and academia to share their unique insights and perspectives on security issues and discuss new approaches and strategies for collaboration. This section highlights the conclusions and recommendations captured from the panel sessions and facilitated discussions at the R&D Exchange. They are offered for consideration by the workshop attendees and the IES.

4.1 Conclusions

The general conclusion of the R&D Exchange was the challenges to securing networks in a converged and distributed environment grow more difficult. Further, those challenges require a greater deal of cooperation amongst network providers, vendors, and users. More specifically, the participants concluded that –

- The shortage of qualified IT professionals, particularly those with expertise in information assurance and/or computer security, remains a major impediment to strengthening the security of the NGN. The participants believed programs, such as the Scholarship for Services program under the Federal Cyber Service initiative and others designed to create financial incentives for students to pursue computer security disciplines at the graduate and undergraduate levels, need to be implemented.

- The IA Centers of Excellence program is an excellent initiative to address the growing demand for computer security professionals but needs to be expanded beyond the current 14 schools. Moreover, a need exists to make information about the IA Centers of Excellence and other IA curricula and certifications available to other schools, such as community colleges and technology trade schools. In addition, participants encouraged cyber ethics training at the K-12 level.

- The Partnership for Critical Infrastructure Security represents an important step in enhancing the relationship between the private sector and the Government, but wider participation by academia and officials in State and local governments is needed.

- Developing a business case for security poses difficult challenges in the commercial sector, and there is a need to offset the high costs and high risks associated with R&D in security technology. Tax credits and other financial incentives might allow companies to minimize their risks and encourage commercial enterprises to increase the funding of security technology R&D.

- Given the complexity introduced to networks by convergence and the proliferation of network providers and vendors, best practices, standards, and protection profiles that ensure security must be evenly applied across the NGN.

- There is a need to enhance R&D efforts to develop better testing and evaluation programs to reduce the vulnerabilities introduced by malicious software. While securing the transmission of voice and data remains an important concern, it is equally important to identify security vulnerabilities in the network control space.

- New types of threats, such as distributed denial of service attacks, challenge corporations to develop security policies and procedures to protect themselves from liability claims. For example, new legal precedents, case law, and Federal legislation such as HIPAA are forcing organizations to take new security measures to protect the confidentiality and integrity of information or risk civil litigation.

- Although technology remains an important component in building security solutions, it is vital to conduct research activities in other areas such as operations, legal and public policy, and human factors. The efficacy of technological solutions is often dependent on the ability of human operators to properly implement, administer, and manage the technology consistent with company policy and the legal constraints.

- There is a need to sponsor joint events like TISW 2000 and the R&D Exchange that facilitate a dialogue among representatives from industry, Government, and academia. All three communities play a crucial role in the R&D of security technologies and applications, and participants described how holding events at universities with IA programs offered unique benefits. Most notably, such events allow security practitioners from industry, Government, and academia to share views and opinions on R&D issues in an informal, research-oriented setting.

4.2 Recommendations

The participants at the R&D Exchange offered several recommendations for consideration by the Government and NSTAC. The thrust of these recommendations is to improve the security of networks in a converged and distributed environment.

The Government should:

- Establish and fund Government programs to encourage increasing the number of graduate and undergraduate students pursuing study in computer security disciplines. Those programs include national initiatives such as the Scholarship for Services program under to the Federal Cyber Services to ensure that the Government educates, trains, and retains access to highly qualified IT security professionals.

- Increase the funding and support to the National Security Agency and other Government agencies to facilitate the certification of additional IA Centers of Excellence to train and educate the next generation of IT security professionals.

- Develop tax credits and other financial incentives to encourage industry to invest more capital in the research and development of security technologies.

- Expand partnerships on critical infrastructure protection issues by encouraging more representatives from academia and State and local governments to participate.

- Invest in R&D programs that encourage the development of best practices in NGN security, such as improved testing and evaluation, broadband protection profiles, and NGN security standards.

To support the Government, the NSTAC should:

- Consider the issues of best practices and standards its report to NSTAC XXIV.

- Consider the legal issues discussed at the R&D Exchange, including linked or third party liability and new privacy legislation and regulations such as HIPAA.

- Conduct another R&D Exchange in the Fall of 2001 in partnership with one or more of the IA Centers of Excellence to continue the dialogue with Government and academia. The purpose of that exchange should be to discuss the difficulties in and strategies for both increasing the number of qualified IT security professionals and enhancing the academic curricula to meet the security challenges of the NGN.

APPENDIX A

R&D EXCHANGE TRACK AGENDA AND ATTENDEES

APPENDIX A
R&D EXCHANGE TRACK AGENDA AND ATTENDEES

Thursday, September 28

SESSION I
Differing Perspectives on Security in Converged Networks
2:00 p.m. – 5:40 p.m.

Keynote Address:
Hon. Curt Weldon, Member, U.S. House of Representatives (R-PA, 7th District)

Moderator:
Peter Fonash, Chief, Technology and Programs Division, National Communications System

Panelists:

Paul Prucnal, Distinguished Professor, Princeton University and HUBS

Edward Balkovich, Director, IP Architecture Systems Engineering, Verizon Communications

Bob Wright, Director, Information Security Management, BellSouth

Dan Woolley, President & COO, Global Integrity Corporation

Jack Edwards, Designated Representative, Nortel Networks

Reception:
Speaker: James Epperson, Jr., President, Southwestern Bell, Oklahoma

Friday, September 29

SESSION II:
Technology Transfer Issues
8:00 a.m. – 9:00 a.m.

Moderator:
Hank Kluepfel, SAIC and R&D Exchange Task Force Chair

Panelists:

Paul Krumviede, Distinguished Technical Member, WorldCom

Gif Munger, Chief System Architect, netEraser, SAIC

SESSION III:
Recap of Main Issues Discussed at TISW 2000 and R&D Exchange
9:00 a.m. – 10:30 a.m.

Panelists:

Hank Kluepfel, SAIC and R&D Exchange Task Force Chair

John Hale, Center of Information Security, University of Tulsa

Terrence Kelly, Senior National Security Advisor, Office of Science and Technology Policy

SESSION IV:
Facilitated Discussion
11:00 a.m. – 12:30 p.m.

Lunch:
Speaker: Del Bothof, President, Applications and Domestic Strategic Investments, Williams Communications

R&D EXCHANGE ATTENDEES
September 28-29, 2000

Name	Organization
Edward Balkovich	Verizon
Dmitry Barinov	Bank of Montreal
Jim Bronson	Sprint
Edward Browdy	DynCorp
Bob Burns	National Telecommunications Alliance
Joe Butcher	Booz•Allen & Hamilton
Scot Cairns	WorldCom
Jan Carroll	Rogers State University
Erin Connor	EWA-Canada
Guy Copeland	Computer Sciences Corporation
Philip Covey	Bartlesville High School
Billie Criss	Williams Communications
Kenneth Davis	Williams Communications
Frank Dixon	NSWC
Jack Edwards	Nortel Networks
H. Eiland	Lockheed Martin
Frank Elim	Sprint
Erick Fabrizio	JAYCOR
Chris Feudo	EDS
Peter Fonash	NCS
Todd Gamble	WorldCom
Irene Gassko	Lucent Technologies
Tim Grance	NIST
Joan Grewe	WorldCom
Richard Groveman	Telcordia
Michael Guard	BankGuard Resources
John Hale	University of Tulsa
Steve Hare	Purdue University
Jack Hagemeister	Washington State University
Ronda Henning	Harris Corporation
Clayton Hoskinson	RCC
Janet Jefferson	NCS
Terry Kelly	Office of Science and Technology Policy
John Kimmins	Telcordia
Hank Kluepfel	SAIC
Paul Krumviede	WorldCom
Righter Kunkel	CyberGuard

Name	Organization
Jim Langster	TV Guide
Clayton Lewis	City of Tulsa
James Longseton	IC Capital
Erin MacDougall	Booz•Allen & Hamilton
Constantine Manikopoulos	NJIT
Dennis McCollum	Williams Communications
Kiesha Miller	NCS
Gif Munger	SAIC
Robert Norris	National Defense University
Kjell Nystuen	Government of Norway
Jack Oslund	Lockheed Martin
Toni Quiroz	US Army CECOM
Greg Parma	NCS
Dave Potter	US Army CECOM
Tim Potter	Rogers State University
D.R. Proctor	CyberGuard
Paul Prucnal	Princeton University
Kevin Pryor	Booz•Allen & Hamilton
Jim Romlein	MIS Labs
Sujeet Shenoi	University of Tulsa
Mary Shumparte	Software Engineering Institute
Marie Stella	FAA
Dave Sulek	Booz•Allen & Hamilton
K. Venugopal	Sprint
Vernon Vogez	DynCorp
Larry Watkins	Williams Communications
Ken Watson	Cisco Systems
Lance Watson	Boston Communications
Greg White	SecureLogix
Chip Whittier	TEDSCO
Dan Woolley	Global Integrity
Bob Wright	Bell South

APPENDIX B

THE TELECOMMUNICATIONS SECURITY TRACK AGENDA
[Sponsored by the National Information Assurance Partnership]

APPENDIX B
THE TELECOMMUNICATIONS SECURITY TRACK AGENDA

Wednesday, September 27, 2000

PLENARY SESSION
8:30 a.m.–10:30 a.m.

Welcoming Remarks:
Robert Lawless, President, University of Tulsa

Tim Grance, Chief, Systems and Network Security Group, National Institute of Standards and Technology (NIST)

Keynote Addresses:
Hon. Richard Clarke, National Coordinator for Counter-Terrorism, National Security Council

Michael Jacobs, Deputy Director, National Security Agency (NSA)

Gary Lytle, Interim President, U.S. Telecom Association (USTA)

Howard Schmidt, Chief Security Officer, Microsoft Corporation

SESSION I:
Security in Convergent Telecommunications and Computer Networks
11:00 a.m. – 12:30 p.m.

Moderator:
Tim Grance, NIST

Presentations:

- *Next Generation Network Security Challenges and Strategies*

John Kimmins, Executive Director, Computer and Network Security Solutions, Telcordia

Network Convergence and Telecommunications Firewalls, Circuit Switched Virtual Private Networks, and Secure Voice over IP
Lee Sutterfield, President and Chairman of the Board, SecureLogix Corporation

- *The Future of Telecommunications*

Mark Bender, Vice President and Chief Information Officer, Williams Communications

Lunch:
Speaker: Gen. Dennis Reimer, U.S. Army (Retired)

SESSION II:
Security Vulnerabilities of Emerging Technologies
2:30 p.m. – 4:00 p.m.

Moderator:
W. Douglas Maughan, Program Manager, Information Technology Office, DARPA

Presentations:

- *Threats and Attacks to Networks*

Bernard Krauss, Vice President, Center for Information Security Technology, Science Applications International Corporation (SAIC)

- *Firewalls for the PSTN*

Gregory White, Vice President Professional Services, SecureLogix

A Look at Security of Voice over IP protocols
Irene Gassko, Lucent Technologies

- *Government Research and Policy Issues for the Converged Network*

Terrence Kelly, Senior National Security Officer, OSTP

SESSION III:
Standards for Telecommunications Security
4:30 p.m. – 6:00 p.m.

Moderator:
Robert Raasch, General Manager, Keane Public Enterprise Consulting

- *Presentations:*

- *NIAP 2000: Protecting the Critical Information Infrastructure*

Stuart Katzke, Chief Scientist, Information Assurance Solutions Group, NSA

- *Telecommunications-Relevant Security Standards within the IETF*

Paul Krumviede, Distinguished Technical Member, WorldCom; Co-chair IETF AAA Committee

- *TIPHON/ETSI VoIP Security Standards - Threats and Solutions*

Stephen Fischer, Director of Business Relations and Standards, Aravox Technologies; Chairman, TIPHON workgroup 8 (Security)

-
-

- *ATM Forum Security Specification Overview*

Richard Graveman, Director, Security Research Group, Telcordia Technologies; Chair ATM Forum Security

Dinner:
Speaker: Hon. Frank Keating, Governor of Oklahoma

Thursday, September 28, 2000

PLENARY SESSION
8:00am -- 9:00am

Welcoming Remarks:
Robert Lawless, President, University of Tulsa

John Sopko, Deputy Assistant U.S. Secretary of Commerce, NTIA

Keynote Addresses:
Harris Miller, President, Information Technology Association of America (ITAA)

William Cook, Partner, Winston & Strawn, Attorneys

SESSION IV:
Security Issues of Network Integration
9:15 a.m. – 10:45 a.m.

Moderator:
Kenneth Davis, Information and Computer Security Coordinator, Williams Communications

Presentations:

- *Achieving COTS Solutions for Telecommunications Critical Infrastructure Protection*

Richard Arnold, Advanced Programs Manager, Information Assurance General Dynamics, Electronic Systems

The Public Switched Network is now Really Public

- *David Henderson, Vice President, Sevis Corporation*
-
- *The Integrated Telecommunications Infrastructure - An Integrator's Perspective*

Ronda Henning, Senior Security Engineer, Government Communications Systems Division, Harris Corporation

SESSION V:
Secure Telecommunications Network Management
11:00 a.m. – 12:30 p.m.

Moderator:
Man-Ho Park, Senior Manager, Network Services Security, WorldCom

Presentations:

- *Managing Security on Network Management Infrastructure*

Kootala Venugopan, Group Manager, Network Security Services, Sprint Communications

- *Are Your Enterprise Management and Security Products Putting You at Risk?*

Kami Brooks, Chief Security Engineer, Emerging Technologies, Averstar*

Managing the Security of a Telecomm Network
Patrick Cain, Security Advocate, CTO Office, Genuity Inc.

Issues in Managing Security for the Telecom Enterprise

- *Joseph Hamblin, Principal Systems Engineer, Tivoli Systems*

Lunch:
Speaker: Hon. Susan Savage, Mayor of Tulsa

APPENDIX C

THE CRITICAL INFRASTRUCTURE PROTECTION TRACK AGENDA
[Sponsored by the National Telecommunications and Information Administration]

APPENDIX C
THE CRITICAL INFRASTRUCTURE PROTECTION TRACK AGENDA

PLENARY SESSION
8:30 a.m. – 10:30 a.m.

Welcoming Remarks:

Robert Lawless, President, University of Tulsa
Tim Grance, Chief, Systems and Network Security Group, NIST

Keynote Addresses:
Hon. Richard Clarke, National Coordinator for Counter-Terrorism, National Security Council

Michael Jacobs, Deputy Director, National Security Agency (NSA)

Gary Lytle, Interim President, U.S. Telecom Association (USTA)

Howard Schmidt, Chief Security Officer, Microsoft Corporation

PANEL I:
Critical Infrastructure Protection (CIP) Practices and Guidelines for Small and Medium-Sized Businesses
11:00 a.m. – 12:30 p.m.

Moderator:
Guy Copeland, Vice President, Information Infrastructure Programs, Computer Sciences Corporation (CSC)

Panelists:

Tari Schreider, Global Operations Manager, Internet Security Systems (ISS)

Stuart Katzke, Chief Scientist, Information Assurance Solutions Group, NSA

Howard Schmidt, Chief Security Officer, Microsoft Corporation

Henry Kluepfel, Vice President, Science Applications International Corporation (SAIC)

Lunch:
Speaker: Gen. Dennis Reimer, U.S. Army (Retired)

PANEL II:
CEO Level Concerns for Legal and Business Consequences of Information
2:30 p.m. – 4:00 p.m.

Moderator:
John Sopko, Deputy Assistant U.S. Secretary of Commerce for Communications and Information, NTIA

Panelists:

David Keyes, Director, Policy, Studies, and Analysis, Veridian Information Solutions

Marshall Sanders, Vice President, Global Security, Level 3 Communications

William Cook, Partner, Winston & Strawn, Attorneys

Hon. David McCurdy, President and CEO, Electronic Industries Alliance; Former Member, U.S. House of Representatives

PANEL III:
Risk Management Process and Risk Assessment —
Tools to Address the Challenge of CIP Interdependencies
4:30 p.m. – 6:00 p.m.

Moderator:
Morgan Wright, iDefense

Panelists:

Commander Stephen Vetter, Deputy Director, CIP Integration Staff, U.S. Department of Defense

Jacques Grenier, Senior Advisor, CIP Task Force, Department of National Defense, Government of Canada

Gregory White, Vice President, Professional Services, SecureLogix

Jeff Dehart, Director, Audit Services, Williams Communications

Dinner:
Speaker: Hon. Frank Keating, Governor of Oklahoma

Thursday, September 28, 2000

PLENARY SESSION
8:00 a.m. – 9:00 a.m.

Welcoming Remarks:
Robert Lawless, President, University of Tulsa

John Sopko, Deputy Assistant U.S. Secretary of Commerce, NTIA

Keynote Addresses:
Harris Miller, President, Information Technology Association of America (ITAA)

William Cook, Partner, Winston & Strawn, Attorneys

PANEL IV:
Case for Partnership:
Defining the Roles of Industry and Government
9:15 a.m. – 10:45 a.m.

Moderator:
Ambassador L. Craig Johnstone, Senior Vice President, U.S. Chamber of Commerce

Panelists:
Robert Miller, Deputy Director, Critical Infrastructure Assurance Office

Kenneth Watson, Alliance Manager, Critical Infrastructure Protection, Cisco Systems

Bernard Farrell, Manager, National Coordinating Center (NCC), National Communications System (NCS)

Harry Underhill, Certified Business Contingency Professional, AT&T; Manager, NCC & NSTAC

Robert Wright, Director, Enterprise Information Security, BellSouth Corporation

PANEL V:
International CIP Policy Perspectives:
Current Approaches to Outreach
11:00 a.m. – 12:30 p.m.

Moderator:
Harris Miller, President, ITAA

Panelists:
Allan MacGillivray, Acting Director, Industry Framework Policy, Industry Canada

Shakil Kidwai, Vice President, Global Information Assurance Services, EDS

James Romlein, President, MIS Labs
Kjell Olav Nystuen, Chief Engineer, Norwegian Ministry of Trade and Industry

Lunch:
Speaker: Hon. Susan Savage, Mayor of Tulsa