
# RESEARCH AND DEVELOPMENT EXCHANGE PROCEEDINGS:

## ENHANCING NETWORK SECURITY TECHNOLOGY R&D COLLABORATION

**A Symposium Sponsored by the President's NSTAC**
**in Conjunction with the Workshop**
**on Security in Large-Scale Distributed Systems**
**Purdue University**
**West Lafayette, Indiana**
**October 20-21, 1998**

***The recommendations contained in this document are being reviewed and considered by the President's National Security Telecommunications Advisory Committee***

## Preface

This proceedings document is a compilation of discussions from the President's National Security Telecommunications Advisory Committee's (NSTAC) third Research and Development (R&D) Exchange. The NSTAC will further review the proceedings and recommendations in preparation for NSTAC XXII and will consider any recommendations arising from this review at that time.

## Acknowledgements

The President's NSTAC extends its thanks to the representatives from industry, government, and academia that participated in the R&D Exchange at Purdue University on October 21, 1998. In particular, NSTAC would like to acknowledge the important contributions of the White House Office of Science and Technology Policy and Purdue University in co-sponsoring this event.

NSTAC also extends its gratitude to Gene Spafford, Steve Hare, Marlene Walls, Andra Short, and the students of Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS), who were instrumental in the planning and conduct of this exchange of ideas on security technology.

# R&D EXCHANGE
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY ..... ES-1**

**1.0 INTRODUCTION ..... 1**

1.1 Background ..... 1
1.1.1 NSTAC Network Security Activities ..... 1
1.1.2 Critical Infrastructure Protection ..... 3
1.2 Scope ..... 3
1.3 Objective ..... 3
1.4 Format ..... 4

**2.0 OBSERVATIONS ..... 5**

2.1 R&D Priorities ..... 5
2.2 Roles of Government, Industry, and Academia ..... 6
2.3 Obstacles ..... 7
2.4 Collaborative Approaches ..... 8

**3.0 CONCLUSIONS AND RECOMMENDATIONS ..... 10**

3.1 Conclusions ..... 10
3.2 Recommendations ..... 11

**APPENDIX A: AGENDAS FROM THE SECURITY IN LARGE-SCALE DISTRIBUTED SYSTEMS WORKSHOP AND THE R&D EXCHANGE ..... A-1**

**APPENDIX B: R&D EXCHANGE ATTENDEES ..... B-1**

**APPENDIX C: R&D EXCHANGE SPONSORS ..... C-1**

## EXECUTIVE SUMMARY

Over the past decade, computer and information security emerged as a complex issue facing our society as it prepares to enter the 21st century. Innovations in information technology have enhanced economic competitiveness, national security, and quality of life improvements. However, these benefits are not without risk. The widespread adoption of information technologies in the private and public sectors has introduced new vulnerabilities into key business and mission critical systems. The proliferation and availability of powerful, user-friendly computer intrusion tools have made it easier for intruders to attack and disrupt these systems. Eliminating vulnerabilities and deterring future threats will require improvements in security technology. The research and development (R&D) conducted by the government, private sector, and academia contribute to improving the security of information systems.

The President's National Security Telecommunications Advisory Committee (NSTAC) sponsored its third R&D Exchange in concert with the White House Office of Science and Technology Policy and the Purdue University Center for Education and Research in Information Assurance and Security (CERIAS). The purpose was to stimulate discussion among security technology practitioners from industry, government, and academia on the need for security technology R&D collaboration. Discussions concentrated on four broad areas: national R&D priorities; the appropriate roles of government, industry, and academia; obstacles; and alternative approaches to collaboration. Discussions at the exchange led to the following conclusions:

- There is a significant "brain drain" occurring in government and academia with respect to computer and network security. Specifically, government and academia are at a distinct disadvantage in competing with industry to secure the services of information security professionals.

- A significant technical impediment to improving security technologies is the lack of metrics to indicate a system's security status, assess risks, and measure performance.

- Another technical impediment is the lack of large-scale testbeds. Participants discussed development of joint or virtual "neutral party" testbeds that allow all organizations—industry, government, academia, or others—to test products in realistic environments.

- Current programs remain concentrated on "respond and react" technologies rather than considering the full range of risk management needs.

- The funding model used by industry and government is not always conducive to taking the long view of security. A short-term, deliverable-driven approach limits the ability of academia to develop long-term programs and to attract and retain faculty.

- Effective industry-government-academia collaborative models exist in disciplines other than information security. Participants discussed the feasibility of an independent clearinghouse to provide organizations interested in security R&D with access to technology, standards, industry best practices, and awareness programs.

- Conference participants emphasized the importance of taking the long view of security, projecting those computer and network security challenges likely to emerge in the next 5-10 years.

The deliberations at the R&D Exchange resulted in several recommendations for consideration by the government and the NSTAC. To improve collaboration among government, industry, and academia and to encourage the development of security tools and products that promote information and infrastructure assurance, the government should consider:

- Identifying potential centers of excellence in academia, industry, and government and providing them with appropriate long-term funding to promote the development of computer security professionals, disciplines, and programs.

- Developing incentives to promote industry investment in long-term security and infrastructure assurance technologies.

- Establishing government programs that encourage undergraduate and graduate students to pursue further study in computer and information security.

- Continuing to incorporate advice from leading experts from the private sector, academia, and advisory boards to assist OSTP as it develops, refines, and implements a national infrastructure assurance R&D agenda.

- Conducting a joint study with NSTAC and academia on the need for, feasibility of, and costs associated with the establishment of large-scale testbeds to: promote joint research, develop and verify metrics, test and evaluate security products, and address other technical needs in network security and information assurance.

To support the government's efforts to develop investment strategies for improving information and infrastructure assurance technologies, participants at the R&D Exchange recommended that the NSTAC should consider:

- Working with the government and academia to study the need for, feasibility of, and costs associated with the establishment of large-scale testbeds to: promote joint research, develop and verify metrics, test and evaluate security products, and address other technical needs in network security and information assurance.

- Examining the business case associated with industry funding student grants, fellowships, and scholarships; sponsoring exchange programs and providing subject matter experts to assist academic programs; and funding endowed teaching positions.

- Conducting another R&D Exchange in the spring of 2000 to continue the dialogue with government and academia and to consider the long-term issues associated with infrastructure assurance and network security, including: new threats; the introduction of new technologies and vulnerabilities; and the convergence of communications and computing technologies.

# Research and Development Exchange Proceedings

## 1.0 INTRODUCTION

The President's National Security Telecommunications Advisory Committee (NSTAC), in concert with the White House Office of Science and Technology Policy (OSTP) and Purdue University, sponsored its third Research and Development (R&D) Exchange on October 21, 1998. That exchange was held in conjunction with Purdue University's Workshop on Security in Large-Scale Distributed Systems. The purpose was to generate discussion among representatives from industry, government, and academia on the need for enhanced information security technology R&D collaboration. This document captures the discussion and observations of the R&D Exchange and identifies several recommendations to maximize the Nation's return on its R&D investments in information security and infrastructure protection technologies.

## 1.1 Background

Global technological leadership is recognized as an essential element of national power. Innovations and advances in technology increase economic vitality, national security, and societal well being. The research and development funded, conducted, and supported by the U.S. Government, the private sector, and academic institutions directly contributes to the Nation's economic, industrial, and technological leadership. Research and development is the systematic study and application of knowledge and is roughly divided into the following categories of technical activities: basic research, applied research, and development.

### *1.1.1 NSTAC Network Security Activities*

The President's NSTAC promotes enhanced network security through its efforts to examine policy and technical issues. Those efforts commenced in 1990, when NSTAC formed the Network Security Task Force to assess the threats posed to the public switched network (PSN) by hackers. That task force identified six technology areas in which government and industry should pursue commercially applicable security tools. In 1991, the NSTAC conducted its first R&D Exchange to provide a forum for industry and government officials to discuss those six technology areas and exchange information about ongoing R&D projects.

In subsequent years, NSTAC broadened its analysis of network security policy and technical issues. A second R&D Exchange was conducted in September 1996 to provide industry and government with an opportunity to develop a common understanding of network security problems affecting national security and emergency preparedness (NS/EP) telecommunications. Four broad areas were identified: authentication, intrusion detection, integrity, and access

control. In its After-Action Report of that exchange, NSTAC determined that regular exchanges should be conducted to identify needs and gaps in ongoing network security R&D and to identify where NSTAC assistance may be warranted. In addition, that report identified the need to consider the notion of a joint industry-government R&D consortium for security technology.

In the fall of 1996, NSTAC conducted a study to examine the issues associated with intrusion detection technology R&D. The resulting report[1] examined several policy, technical, and human factors affecting the development, implementation, acceptance, and management of intrusion detection systems. Central to that report was the notion that managing security occurs across a broad spectrum of actions, as depicted in Figure 1.

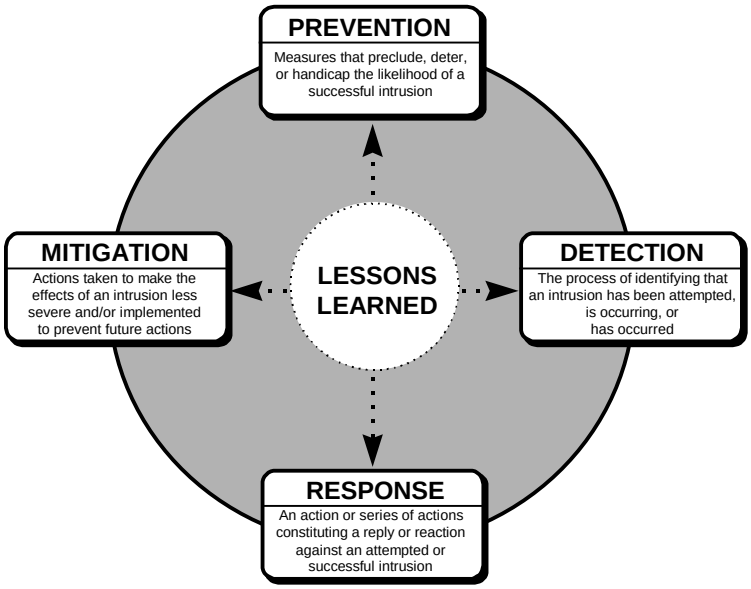


*Figure 1*

The Intrusion Detection Subgroup report also reinforced prior recommendations to examine the need for and feasibility of collaborative R&D approaches (e.g., consortium, joint testbeds) for security technology. That topic was selected as the theme of the next R&D Exchange.

[1] "Report on the NS/EP Implications of Intrusion Detection Technology Research and Development", President's National Security Telecommunications Advisory Committee, December 1997.

### *1.1.2 Critical Infrastructure Protection*

Another impetus for increased attention on R&D in the area of information and security technologies was the emergence of the critical infrastructure protection issue. On July 15, 1996, President Clinton signed Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP). The primary purpose of the PCCIP was to examine the vulnerability of the Nation's critical infrastructures to physical and "cyber" threats. The Commission identified new concerns, specifically in the context of potential adversaries using advanced information technologies to attack our Nation's critical infrastructures. Those infrastructures are more vulnerable than in the past because they increasingly depend on open and interconnected computer systems to manage their critical business processes. In its October 1997 report, *Critical Foundations*, the PCCIP acknowledged the vital importance of R&D in combating the emergence of these types of threats and recommended a significant increase in R&D funding for infrastructure protection technologies.

On May 22, 1998, President Clinton signed Presidential Decision Directive 63 (PDD-63). That document outlined a national policy with the intent of eliminating significant vulnerabilities in critical infrastructures. Improved technologies through national R&D programs are identified as a key element of this strategy. The federal government is currently developing and refining an infrastructure assurance technology roadmap to support that national strategy. OSTP and a federal interagency working group composed of representatives from federal lead agencies are identifying, prioritizing, and determining funding for the R&D of infrastructure assurance technologies for each critical infrastructure.

## 1.2 Scope

This document focuses on the discussions and observations distilled from the 1998 R&D Exchange. In addition, it includes concepts and ideas first surfaced at the Workshop on Security in Large-Scale Distributed Systems sponsored by Purdue University on October 20, 1998. Many of the invitees to the R&D Exchange also participated in this workshop and there was considerable dialogue on the need for enhanced collaboration.

## 1.3 Objective

The primary objective of the R&D Exchange was to foster a dialogue among industry, government, and academia on approaches to improve security technologies. The agenda for the exchange was driven by two themes:

- *Network Convergence* - There are numerous network security issues associated with the convergence of telecommunications networks and the Internet. With each passing

year, the boundaries separating telecommunications service providers and Internet service providers grow more difficult to define.

- *Collaboration* - Maximizing the Nation's R&D investments in security technologies will require collaboration among industry, government, and academia. Given growing national concerns about risks posed to critical infrastructures, a well-defined approach to R&D is a national imperative.

For the most part, the R&D Exchange focused on the issue of collaboration. However, issues of network convergence were discussed as part of the October 20 workshop.

### 1.4 Format

The R&D Exchange was held in conjunction with the Workshop on Security in Large-Scale Distributed Systems, which focused on security technologies, security policy and management, and incidents and investigations. The R&D Exchange was an invitation-only session to discuss mechanisms for collaboration. The session commenced with presentations from each of the three communities:

- *A View from Industry* – Mr. Guy Copeland, Computer Sciences Corporation
- *A View from Government* – Dr. Steven Rinaldi, OSTP
- *A View from Academia* – Dr. Eugene Spafford, Purdue University

Each representative provided a brief overview addressing the following questions:

- What are the long-term security technology R&D objectives and priorities?
- What are the respective roles of industry, government, and academia to accomplish these objectives?
- What are some major obstacles to achieving those objectives?
- How will collaboration be achieved to satisfy those objectives?

The remainder of the R&D Exchange was devoted to a roundtable discussion of those topics. The conference agenda is attached as Appendix A. A list of the conference attendees is attached as Appendix B. A description of the conference sponsors is provided in Appendix C.

## 2.0 OBSERVATIONS

This section describes the discussions and observations from the R&D Exchange. Those observations were captured on a non-attribution basis. It should be noted that many of the observations from the R&D Exchange were consistent with the findings and recommendations from the NSTAC's December 1997 Intrusion Detection Subgroup (IDSG) Report.[2]

### 2.1 R&D Priorities

The first issue the participants discussed was long-term information and infrastructure security technology R&D objectives and priorities. Underlying this discussion were two interrelated tensions. The first was the need to focus on long-term R&D objectives while simultaneously recognizing the dynamic forces of technological innovation. Although there was general agreement on the need for longer "time horizons" on R&D projects, the participants also acknowledged that rapid laboratory-to-market cycles in the private sector provided significant challenges. The second tension was the role of market forces in establishing an appropriate balance between profitability, availability, security, reliability, and resiliency. It was acknowledged that organizations are often reticent to invest in security, which diverts funds from other organizational priorities like delivering new products and services to market. In addition to these tensions, conference participants identified three R&D priorities:

- *Metrics* – A consistent theme was that developing realistic metrics to measure the effectiveness of security programs is crucial. Several representatives emphasized that metrics are the means by which viable business cases are developed and communicated with senior managers in all types of organizations. Security managers can use metrics to rationalize increased investment in security and to validate an organization's level of success and performance. Metrics can also help security managers identify the true nature of the threat to information systems (e.g., are the threats primarily "insiders" or do most intrusions come from outside the organization?)

- *Managing Risk* – A general observation in both sessions was that too much emphasis is placed on the development of "response or react" technologies. Several representatives suggested broadening the R&D focus to include the entire spectrum of risk management. This includes technologies that prevent or deter intrusions; technologies and methodologies to support recovery and reconstitution; and training employees (see below). For instance, it was suggested that many organizations devote considerable efforts to developing technologies to support the detection and

[2] The Intrusion Detection Subgroup report identified three factors requiring attention: national policy, technological development, and the human element. Many of the IDSG report's findings are parallel to the observations from the R&D Exchange.

response to an incident. In some cases, those same organizations fail to develop robust architectures that take security into account or neglect to implement basic security precautions. Similarly, it was noted that research into systems and tools to support recovery and reconstitution is limited.

- *Education, Training, and Awareness* – It was acknowledged that one of the most difficult challenges facing all organizations is educating and training employees and making them more aware of security risks. Poor training and education can lead to significant implementation and management problems when new security technologies are introduced. Developing R&D programs that recognize the importance of the human aspects of security was identified as a priority. This also suggests a need to vertically apply the security discipline into traditional computer science and engineering disciplines.

## 2.2 Roles of Government, Industry, and Academia

A major issue considered by the participants was the question of the proper roles of government, industry, and academia in promoting collaborative relationships in security technology R&D. Specifically, the participants discussed the roles of:

- *Government* – Participants suggested an appropriate role for the federal government is to consider the social good and to adopt the long view of R&D. This included both basic research and applied development. The federal government possesses numerous strengths, most notably the financial resources to fund and support technologies where a viable market has yet to develop.

- *Industry* – Participants agreed the appropriate role for industry is to lead in applied development. Industry is able to leverage resources (financial, personnel) for those technologies with commercial applicability. A key discussion point was the need for industry to provide academia with opportunities—through direct funding, technology transfer, or exchange programs—to train new professionals in the fields of network and information security. Another discussion thread was the possible role of the insurance industry in providing "incentives" for improving security.

- *Academia* – Participants suggested that an appropriate role for academia is to take the lead in basic research and to train future professionals in the field. Academia has the ability to focus on both near- and long-term research, but requires a stable source of funding to build programs and centers. A concern expressed in the R&D Exchange was that academia lacks sufficient resources to build networks and systems that adequately replicate those being used in the private sector. In addition, it was noted that academia is being attracted to more applied research with direct commercial applications than it has traditionally been.

## 2.3 Obstacles

Participants identified the following obstacles to achieving R&D collaboration:

- *Funding Models* – A significant theme was the different funding models used by industry, government, and academia. Conference participants commented that industry investments are driven by short-term (6-12 months) objectives and the results are not often shared for competitive reasons. Government develops budgetary cycles two or three years in advance and focuses on deliverable-driven project schedules. Academia relies on both sources of funding to augment its programs. However, the short-term nature of both industry and government provides considerable challenges to academia. First, these monies are usually provided on a year-to-year basis, making it difficult to build programs, hire professors, recruit students, and buy equipment. Second, the schedules are deliverable-driven–as one representative noted, "it is difficult to innovate on schedule." Third, some representatives expressed concern that government funding is often delayed, which can present financial problems, such as paying faculty and providing scholarships and fellowships to students.

- *Scarce Pool of Professionals* – Another theme was a universal concern about the limited availability of security professionals. Industry needs these people to manage, administer, and secure their increasingly complex networks. Government requires similar personnel to support national security and law enforcement missions. Academia requires them to teach undergraduate and graduate students and to conduct research. As demand grows—and consequently salaries and other benefits–both government and academia face a significant "brain drain" of professionals in network and information security disciplines.

- *Valuation of Security* – A key discussion topic was that security costs tend to be concentrated within an organization whereas the benefits of security programs are diffuse and distributed. With increasingly interconnected networks, these benefits extend well beyond the organization itself. This makes it difficult for managers and security practitioners to demonstrate the value or importance of their activities to the overall success of the organization. Complicating matters, organizations typically have similar problems in valuing information—for instance, how does an organization account for the loss of a piece of intellectual capital? While already identified as an R&D priority, the lack of standardized metrics and other techniques limits the ability of these managers to measure performance and justify greater investments in security tools, techniques, and personnel.

- *Lack of Testbeds* – As networks and systems grow more complex, conducting tests and experiments becomes increasingly difficult and expensive. It is usually beyond

the means of universities to realistically replicate large networks consisting of hundreds of systems and nodes. Similarly, individual companies and government organizations do not have sufficient resources to establish large-scale networks dedicated to testing and experimentation. It was noted that this limits the ability of organizations to develop scalable information security solutions.

## 2.4 Collaborative Approaches

Finally, the participants discussed possible means for R&D collaboration to improve information security and infrastructure protection technologies. Specific approaches included:

- *Clearinghouse* – Several representatives discussed the need for a clearinghouse to foster and facilitate the exchange of information on education programs, outreach initiatives, awareness, best practices, and test-case scenarios to test new products, services, and technologies. It was also discussed that a clearinghouse might serve to develop comprehensive security metrics for use by industry, government, and academia.

- *Centers of Excellence* – Another collaborative approach identified in the R&D Exchange was university-based centers of excellence. These centers are more able to attract faculty interested in research, high caliber students, and industry support and endowment. They can partner with industry centers of excellence and research laboratories and the government's national laboratories. In addition, it was noted that there are several existing "centers of excellence." An example cited was the Government-Industry Cooperative Research Institute, which was established via a partnership between the Department of Defense and the Electric Power Research Institute.

- *Exchange Programs* – A third approach discussed was the concept of exchange programs. One such program was discussed at the R&D Exchange. The National Security Agency has a fellowship program that funds selected individuals to spend three years working in industry and academia. This has two important benefits. First, it provides the government with a more technically knowledgeable individual. Second, it provides academic institutions with a unique expertise in developing course materials and practical applications of theoretical concepts.

- *Joint and Virtual Testbeds* – Several representatives discussed the need to develop joint and/or virtual testbeds. One suggestion was to establish a network of user and testing facilities of companies that would volunteer resources while academia provides researchers. This could be mutually beneficial to both parties because academia can gain access to advanced networks that would be too expensive to build whereas industry could use these relationships to recruit technically knowledgeable

employees. Another suggestion was the creation of virtual networks operated by multiple companies, also referred to as neutral party testbeds.

## 3.0 CONCLUSIONS AND RECOMMENDATIONS

This section describes the conclusions and recommendations derived from the discussions at the R&D Exchange.

### 3.1 Conclusions

The primary conclusion from the R&D Exchange was that the continued exchange of views and dialogue between industry, government, and academia is crucial as the Nation begins efforts to address infrastructure protection issues through R&D investments in security technologies. This was the first time academia was invited to participate in the R&D Exchange, and their views proved insightful and valuable.

More generally, the participants concluded that:

- There is a significant brain drain occurring in government and academia with respect to computer and network security. Specifically, government and academia must compete with industry to secure the services of information security professionals but are at a distinct disadvantage given their limited resources.

- A major technical impediment to improving security technologies is the lack of metrics to indicate an organization's or system's security posture. Metrics play an important role in the context of assessing risks, evaluating new security tools and products, developing professional accreditation and standards, and quantifying the value of security in organizations.

- Another technical impediment is the lack of testbeds. Participants discussed the possibility of developing joint or virtual "neutral party" testbeds that allow all organizations—industry, government, academia, or others—to develop and test products and train students and employees in realistic environments.

- Current programs remain concentrated on respond and react technologies rather than considering the full range of risk management needs. An R&D agenda that includes technologies to prevent intrusions and reconstitute systems in the aftermath of an intrusion would provide a more balanced and comprehensive approach to addressing security needs.

- The funding models used by industry and government are not always conducive to taking the long view of security. A short-term, deliverable-driven approach limits the ability of academia to develop long-term research programs and methodologies and to attract and retain dedicated faculty. The establishment of viable academic

programs—and robust centers of excellence—requires a more stable source of funding.

- Effective industry-government-academia collaborative models exist in disciplines other than information security. Conference participants emphasized the importance of establishing an independent clearinghouse to provide organizations interested in security R&D with access to technology, standards, industry best practices, test-case scenarios, and awareness programs. This conclusion is consistent with the findings of the NSTAC's National Information Infrastructure Task Force in examining the need for and feasibility of an Information Systems Security Board (ISSB).[3]

- Conference participants emphasized the importance of taking the "long view" of security, projecting those computer and network security challenges likely to emerge in the next 5-10 years.

### 3.2 Recommendations

The deliberations at the R&D Exchange resulted in several recommendations for consideration by the government and the President's NSTAC. To improve collaboration among government, industry, and academia and to encourage the development of security tools and products that promote information and infrastructure assurance, the government should consider:

- Identifying potential centers of excellence in academia, industry, and government and providing them with appropriate long-term funding to promote the development of computer and network security professionals, disciplines, and programs.

- Developing incentives (e.g., revisions of capital gains tax policy) to promote industry investment in long-term security and infrastructure assurance technologies.

- Establishing government programs that encourage undergraduate and graduate students to pursue further study in computer and information security.

- Continuing to incorporate advice from leading experts from the private sector, academia, and advisory boards to assist OSTP as it develops, refines, and implements a national infrastructure assurance R&D agenda.

[3] "National Information Infrastructure Task Force Report," President's NSTAC, March 1997. The task force conceptualized the ISSB 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.

- Conducting a joint study with NSTAC and academia on the need for, feasibility of, and costs associated with the *establishment of large-scale testbeds* to: promote joint research, develop and verify metrics, test and evaluate security products, and address other technical needs in network security and information assurance.

To support the government's efforts to develop investment strategies for improving information and infrastructure assurance technologies, participants at the R&D Exchange recommended that the NSTAC should consider:

- Working with the government and academia to study the need for, feasibility of, and costs associated with the *establishment of large-scale testbeds* to: promote joint research, develop and verify metrics, test and evaluate security products, and address other technical needs in network security and information assurance.

- Examining the business case associated with industry funding student grants, fellowships, and scholarships; sponsoring exchange programs and providing subject matter experts to assist academic programs; and funding endowed teaching positions.

- Conducting another R&D Exchange in the spring of 2000 to continue the dialogue with government and academia and to consider the long-term issues associated with infrastructure assurance and network security, including: new threats; the introduction of new technologies and vulnerabilities; and the convergence of communications and computing technologies.

# APPENDIX A

## AGENDAS FROM THE SECURITY IN LARGE-SCALE DISTRIBUTED SYSTEMS WORKSHOP AND THE R&D EXCHANGE

Proceedings from the Workshop on Security in Large-Scale Distributed Systems

**KEYNOTE PRESENTATION:** HANK KLUEPFEL, SAIC

**SESSION I: TECHNOLOGY**

An Efficient MPEG Video Encryption Algorithm
*C. Shi, B. Bhargava*

Security in the Large: Is Java's Sandbox Scalable?
*Q. Zhong, N. Edwards*

**SESSION II: POLICIES AND MANAGEMENT ISSUES**

Enforcing Security Policies in Large Scale Communications Networks
*T.K. Apostolopoulos, V.C. Daskalou, S.K. Katsikas, K.D. Moulinos*

Managing Network Security—A Pragmatic Approach
*R. Falk, M. Trommer*

Requirements for a True Enterprise-Wide Security Infrastructure
*D.C. Merrill, A. MacWillson, G. Loveland*

Security in Mobile Systems
*V. Subramanyam, A. Joshi*

**SESSION III: INCIDENTS AND INVESTIGATIONS**

Local Area Detection of Incoming War Dial Activity
*E. Amoroso, E. Kogan, B. McAnderson, D. Powell, B. Rexroad, S. Schuster, A. Stramaglia*

Cyber-Intrusion Response
*R. Brackney*

Legal Reliability in Large-Scale Distributed Systems
*P. Sommer*

R&D Exchange Agenda

| | |
|---|---|
| 8:00-8:45 a.m. | Continental Breakfast |
| 8:45-9:30 a.m. | Tour of CERIAS |
| 9:30-9:35 a.m. | Introductory Remarks<br>*Richard Swanson, CSC* |
| 9:35-9:45 a.m. | Industry Perspective on R&D Collaboration<br>*Guy Copeland, CSC* |
| 9:45-9:55 a.m. | Government Perspective on R&D Collaboration<br>*Steve Rinaldi, OSTP* |
| 9:55-10:05 a.m. | Academic Perspective on R&D Collaboration<br>*Gene Spafford, Purdue University* |
| 10:05-10:30 a.m. | Facilitated Discussion |
| 10:30-10:50 a.m. | BREAK |
| 10:50-11:50 a.m. | Facilitated Discussion |
| 11:50-12:00 p.m. | Closing Remarks / Wrap-Up |
| 12:00 p.m. | Adjourn |

# APPENDIX B

# R&D EXCHANGE ATTENDEES

## October 21, 1998

| NAME | ORGANIZATION |
|---|---|
| Dr. Mikhail Atallah | Purdue University |
| Mr. Robert Burns | National Telecommunications Alliance |
| Ms. Patricia Burt | Department of Commerce |
| Mr. Mark Centra | National Communications System |
| Mr. Guy Copeland | Computer Sciences Corporation |
| Mr. John Davis | National Security Agency |
| Dr. Deborah Frincke | University of Idaho |
| Mr. Tom Fuhrman | Booz·Allen & Hamilton |
| Mr. Peter Gleitz | Department of Defense |
| Mr. Steve Hare | Purdue University |
| Mr. Charles Holland | Department of Defense |
| Mr. David Isacoff | Department of Defense |
| Mr. Hank Kluepfel | SAIC |
| Dr. J. Timothy Korb | Purdue University |
| Mr. Thomas Longstaff | CERT Coordinating Center |
| Dr. John McHugh | Portland State University |
| Mr. Kevin McMahon | MCI Worldcom |
| Dr. Biswanath Mukhejee | University of California at Davis |
| Dr. Steve Rinaldi | Office of Science and Technology Policy |
| Ms. Paula Scaglini | Argonne National Laboratory |
| Dr. E. Eugene Schulz | Global Integrity Corporation/Purdue University |
| Dr. Eugene Spafford | Purdue University |
| Mr. David Sulek | Booz·Allen & Hamilton |
| Dr. S. Samuel Wagstaff | Purdue University |

# APPENDIX C

# R&D EXCHANGE SPONSORS

## THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

The NSTAC is a Presidential Advisory Committee established in September of 1982 to provide advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) telecommunications policy. The NSTAC consists of up to 30 senior corporate leaders representing major telecommunications and information system industries. Those leaders provide the President with a unique source of expertise not available in the Government. The NSTAC offers Federal departments and agencies an opportunity to tap into a vast amount of telecommunications and information technology expertise. The NSTAC maintains several active working groups to examine policy and technical issues associated with NS/EP telecommunications.

## OFFICE OF SCIENCE AND TECHNOLOGY POLICY

The Government plays a critical role in maintaining American leadership in science and technology. In 1976, the Office of Science and Technology Policy was created to provide the President with timely policy advice and to coordinate the Nation's science and technology agenda. OSTP has assumed a prominent role in advancing the Clinton Administration's agenda in fundamental science, research, and technology; education and scientific literacy; and international cooperation. The National Science and Technology Council (NSTC), established by Executive Order in November 1993, plays a key role in developing and executing the Administration's science and technology agenda. This Cabinet-Level Council coordinates the diverse parts of the Federal R&D enterprise and prepares R&D agendas that are integrated across Federal agencies to form an investment package aimed at accomplishing multiple national goals.

## CENTER FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY
**Purdue University**

The Center for Education and Research in Information Assurance and Security (CERIAS) provides innovation and leadership in technology for the protection of information and information resources, and in the development and enhancement of expertise in information assurance and security. The Center is multidisciplinary in nature and addresses the problems of information protection from a variety of different perspectives. These perspectives include research, development, and education in: computer and network security; information security public policy; information management; social, legal, and ethical aspects of information use and abuse; the economics of information assurance; electronic commerce security; risk management; awareness and training methods for information security professionals; computer crime investigation and response; and information warfare issues.