

SUMMARY OF DISCUSSIONS AT A PLANNING MEETING ON

CYBER-SECURITY AND THE INSIDER THREAT TO CLASSIFIED INFORMATION

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD
THE NATIONAL RESEARCH COUNCIL
THE NATIONAL ACADEMIES

NOVEMBER 1-2, 2000

Chair:

**Anita K. Jones, Lawrence R. Quarles Professor of Engineering and Applied Science
University of Virginia**

Rapporteur:

**Lynette I. Millett, Program Officer and Study Director
Computer Science and Telecommunications Board**

This white paper summarizes the discussions of a planning meeting sponsored by the National Research Council (NRC) on November 1-2, 2000. It has not been reviewed by the National Research Council and does not reflect the institutional views of the NRC in any way.

CYBER-SECURITY AND THE INSIDER THREAT TO CLASSIFIED INFORMATION

In order to determine whether to conduct a study on cyber-security and the insider threat to classified information, the Computer Science and Telecommunications Board (CSTB) of the National Academies (described in Appendix A) hosted a meeting on November 1-2, 2000 to advise CSTB on the issues that such a study might address.

Meeting participants endorsed the concept that CSTB should undertake a project that would examine high-grade threats (by definition including insider threats) to high-value information systems. Such a study should focus both on national security concerns and classified systems as well as non-classified, commercial enterprises.

The meeting was chaired by Anita K. Jones, Lawrence R. Quarles Professor of Engineering and Applied Science, the University of Virginia. The steering committee consisted of Tom Bozek, Office of the Secretary of Defense; Michael Caloyannides, Mitretek Systems; and Carl Landwehr, Mitretek Systems. Meeting participants (Appendix B) included experts in information security, law, national defense, and law enforcement. The meeting agenda is given in Appendix C.

1. Introduction

Public attention to information security today tends to focus on the problem of preventing harm that results from the actions of a hostile “outsider,” such as a hacker. However, security breaches accomplished with the cooperation of (or at the instigation of) an insider can cause significant damage. For example, an insider might be able to disable certain network security mechanisms, thereby allowing a collaborator on the outside to gain access. Or, an insider might be able to transmit electronically large volumes of sensitive information without ever being subjected to physical search. The compromised or actively hostile insider clearly presents a difficult challenge for the manager or security practitioner.

The classic insider attack in which an individual uses authorized access to a computer system to view a sensitive piece of information, memorizes it, and then divulges it at a future date in a different location seems impervious to straightforward technological solutions. However, it may be possible to develop technologies that can mitigate the damage done when such individuals use technological means to assist in the information transfer or are more interested in sabotage than espionage. Technology can also be employed that increases the likelihood that the individual will be caught. Nevertheless, dealing with the insider threat inevitably involves organizational policies, practices, and processes as well as technological approaches. For example, in an environment in which most employees are trustworthy, what policies, practices, and processes can be implemented that will help to cope effectively with the insider threat?

The CSTB meeting’s initial focus was on the threat to classified systems and information because the political and organizational issues that often arise with protection policies and practices (e.g., rights to privacy) are considerably fewer and less intense than if

sensitive unclassified information (especially non-governmental information) is involved. (The reason is that individuals granted access to classified information routinely sign away many rights to privacy that most people take for granted.) During the course of the meeting, however, participants often expanded the discussion to include threats other than insider threats and to include systems other than classified systems. Reasons for this expansion are explored in the next section.

Participants also repeatedly emphasized the fact that security (be it in a classified or unclassified environment) is not simply a matter of appropriate technology application. There are psychological, social, managerial, and legal issues that manifest themselves. These issues are elaborated upon in section 3. Any security solution is a mixture of technology and of people following well-designed procedures. Some of the technological approaches that may prove helpful are discussed in section 4. Section 5 outlines possible suggested next steps for CSTB.

2. High-Grade Threats and High-Value Targets

Meeting discussions made clear that the distinction between classified and unclassified systems was artificial from the point of view of both the technology and, in many cases, the threat. The participants concluded that the focus should be on high-grade threats against high-value targets. These targets may be classified or unclassified, but they have the property that they tend to attract attacks by organizations (including nations) that are well planned, well funded and sustained if necessary. High-value targets also have the property that they are worth the expense of protecting them in whatever way is technically and managerially feasible.

In an attempt to elucidate what is meant by the terms 'high-value target' and 'high-grade threat,' the participants discussed the relevant differences between threats to classified and non-classified information, the differences between the systems themselves, and how such differences might have an impact on the approaches taken to combat the threat. They noted that the fundamental issue is the value of the information. Corporations protect highly sensitive and valuable information, just as the government does. Such non-governmental, non-classified, highly sensitive information (for example, an individual's medical records or a pharmaceutical company's drug research data) is deserving of strong protection.

The anticipated threats will have an impact on what kind of protective measures (both in the research community and in the practitioner community) need to be undertaken; significant threats (sometimes by the same adversary) are now made against both the government ('traditional' espionage) and against corporations (industrial espionage). These threats may well involve insiders, but participants were reluctant to focus exclusively on insiders, due in part to the difficult boundary and definitional problems raised by the use of the term (see section 3). Participants spent some time attempting to characterize the problem in a way that would encompass a broad set of significant attacks while remaining constrained enough not to include all attacks on information systems of any sort.

Distinctions between classified and unclassified systems were discussed and include the following:

- The motivations for attacking classified systems are often much more serious (e.g., personal conviction, blackmail, ideological shifts) than for attacking other systems. Persons may be coerced or recruited, trained, and planted as moles.
- Threats to classified systems often differ from other kinds of threats. A serious threat to classified systems, for example, is espionage stemming from foreign intelligence. Rather than focusing exclusively on attacks that can be executed through the Internet, insiders may be subverted or backdoors may be built into software products. Such attackers have time, patience, and resources.
- While systems within the Department of Defense are mandated to use commercial off-the-shelf (COTS) products, there are processes within government that slow down both upgrades (so that internal users are frustrated at not having the latest software functionality) and patch applications (compromising security). Participants suggested that this problem was more pernicious than in the private sector.
- The degree of testing varies between types of systems. Unclassified systems in the federal government are subject to less stringent testing than classified systems.

Notwithstanding these distinctions, there are also several similarities between the classified and non-classified spheres of influence. Information inference through data aggregation is a threat to national security as well as to corporate interests. The Department of Defense (DOD) Website, for example, has approximately 200 gigabytes of publicly accessible data from which much could be inferred. In some cases, conclusions that can be drawn might be classified while the individual pieces of data are not. Similarly, sensitive information about a corporation's status or plans can be inferred from disparate pieces of information that are publicly accessible. The increasing amount of information that is easily publicly accessible in electronic form exacerbates this risk.

Classified and non-classified systems alike are subject to both espionage and sabotage. In some cases, access and information (espionage) may be more valuable to the attacker than causing actual damage (sabotage); in others, sabotage might be the goal. The sabotage or compromise of even unclassified networks can have national security implications since significant amounts of sensitive information are transferred over public networks. Much of the United States' critical infrastructure is increasingly dependent upon unclassified networks for operations, which can have a large impact on national security as well.

In light of all of this, participants emphasized that attention needs to be paid to high-grade threats to both classified and non-classified information systems and that too much attention is currently given to lesser threats where solutions are often known but not implemented. A strong case was made that advocacy from the point of view of the high-grade target that receives high-grade threats is needed. In other words, serious security threats require serious attention on the part of the larger research and practitioner community. Any such efforts should encompass classified systems (national security

implications) as well as commercial systems (industrial espionage). With current trends, the overlap between systems with national security implications and commercial systems will grow. The “insider” remains an intrinsic part of this problem, since high-value targets will be attacked no matter what controls are placed on them, and those attacks may often be accomplished through the actions of insiders.

3. Psychological, Social, Legal and Managerial Aspects of the Insider Threat

Meeting participants discussed a number of issues related to the intersection of psychology, sociology, and management policy that affect how best to combat the insider threat to information systems. The first concerns the definition of the term ‘insider’ and methods for understanding the motivations of persons who present an insider threat. The second is the pressing need for more data in this area. The third addresses the complexity of managing employees who are often working with seemingly contradictory or unclear goals (for example, managers who encourage substantive inter-group or inter-institutional collaboration while insisting on protection of sensitive information). The fourth concerns the legal issues that arise with respect to insider security concerns.

Differing Categories of and Motivations for Insiders

Participants acknowledged that defining the term ‘insider’ is difficult.¹ Persons who constitute insider threats range from incompetent users making critical mistakes to moles who have been recruited, trained, and planted by nefarious outsiders; their motivations also vary widely and include the desire for recognition for hacking skills, ideological convictions, and monetary incentives. Determining what techniques are most appropriate in defending against the insider threat requires the consideration of at least three dimensions: the individual’s access privileges, their intent, and their technical abilities.

Need for Data and Modeling Techniques

A compelling case was made at the meeting for the need for more data on insider threats and better modeling techniques. Models of a typical ‘hacker’ have been available for a long time; while similar kinds of composites of persons likely to present an insider threat would also be useful, the requisite repository of data does not yet exist. One challenge to constructing the models and compiling the data needed for such a repository is the fact that insiders can be characterized in many different ways. For example, the behavior of the insider will likely vary depending on a wide variety of factors, including whether that person is unwitting, incompetent, coerced, vengeful, and so on. Such factors imply that simply relying on externally observable traits and behaviors in order to identify potential insiders may not prove useful.

An additional point was made at the meeting about the need for hard data on insider attacks. The salient question to be answered satisfactorily before any particular organization will contribute large numbers of resources to solving the insider threat is: What is the threat, both in terms of number of occurrences and in potential risks or losses

¹ One possibility that was brought up is to consider malicious *code* that mistakenly becomes authorized to be an ‘insider’ of a sort. For the purposes of this summary, the term insider usually referred to a person, however.

per occurrence? Financial institutions, for example, are required to report such information, but very few others do. In recent years, however, the opportunities for profit through attacks on information systems seem to have proliferated. Participants emphasized that more investigation is needed before meaningful answers to this sort of question will be possible.

A suggestion was made to examine case law in areas such as fraud or other classes of misbehavior that are similar to or include insider attacks on information systems. The challenge here is that, for reasons ranging from settlements out of court to unverifiability, the data is not always readily available or accessible. Further, there are, in fact, reasons not to make that data available on the part of those who have been compromised. Even military base commanders may not generally report their insider problems, for example. Banks also are loathe to disclose insider security breaches for obvious reasons. Information Sharing and Analysis Centers (ISACs)² (the Financial Services ISAC³ is an example of one) may prove helpful in gathering and exchanging information.

Within the DOD and other parts of the government that relate to national security, psychophysiology detection (polygraph) is reportedly one of the best investigative tools. It does have limitations, however. The accuracy of the screening exam is around 84%. In addition, polygraph exams can only provide information on events that have taken place in the past; they are unable to provide information about *intent*. Further, there is a limited number of polygraph examiners, which makes widespread use of this tool within the DOD infeasible. More generally, use of the polygraph test is not accepted in the corporate world.

These and other observations led some at the meeting to put forth an argument that focusing on the individual rather than the act itself is problematic in both the government and in the private sector. Spies, broadly speaking, have always existed and it is highly unlikely that means for detecting potential spies will be developed; therefore barriers to particular *acts* are necessary instead. Others suggested that learning to infer behavior and intent from usage signatures could be very powerful, although it is not clear how to achieve that at this point. Furthermore, any such techniques inevitably run the risk of incorrectly labeling problematic behavior acceptable, or, arguably worse, determining benign usage signatures to be indicative of inappropriate behavior or intent.

Management Issues

The structure of the workplace today produces challenges for managers who are attempting to minimize risks and maintain system security. One observation made was the need for better training and security awareness education. This could be especially helpful in the case of the unwitting insider or the incompetent user. An effort on the part of management to find ways to motivate people not to do 'bad things' might also be

² An ISAC is a private sector entity that facilitates the collecting and sharing of incident and response information among its members as well as information exchange between government and the private sector. ISACs were promoted by the Critical Infrastructure Assurance Office (<http://www.ciao.gov/>) in response to the President's Commission on Critical Infrastructure Protection's 1997 report *Critical Foundations: Protecting America's Infrastructures* (http://www.ciao.gov/PCCIP/report_index.html).

³ <http://www.fsisac.com/>

effective. Taking into account psychological profiles when hiring is another tactic; this can be problematic though, especially without consistent metrics to distinguish merely quirky employees from potentially dangerous individuals. Research into organizational and functional work design as it pertains to making it easier (or possible) to audit activities that would reveal undesirable insider activities was also mentioned as a way to provide management with better tools to address the problem. The broad implications of employee monitoring were not discussed.

Recent movements toward more open architectures along with more collaboration and teamwork within and across institutions present even more management challenges. In a classified environment, for example, information is supposed to be distributed on a need-to-know basis, but given a shift towards more collaborative exercises, determining who needs to know what and constraining the sharing of information to that end is difficult. Similarly, in the business world, there has been a significant movement toward embracing cooperation across organizations and sectors, but this, of course, introduces security problems. One participant characterized the dilemma in both domains by paraphrasing directives from senior management and government as, “Collaborate with everybody but build systems that are resistant to attack.”

Legal Issues

There are many legal aspects to the problem of the insider threat. First, the usual privacy and workplace surveillance issues need to be addressed when determining how, within an organization, to implement tools to decrease the possibility of insider malfeasance. In addition to this, though, is the issue of building technology that produces data (audit logs, for example) that meet acceptable legal and forensic standards. The interplay between employment laws and the need for system security is also a concern. For example, termination of suspected individuals may not occur immediately, and thus such people may maintain access to sensitive information while the necessary paperwork goes through channels. Finally, sophisticated adversaries can take advantage of jurisdictional differences and route their attacks through non-cooperating jurisdictions. The jurisdictional challenges are complicated by the fact that under U.S. law search warrants are geographical in nature.

4. Technology, Present and Future

Participants in the meeting discussed several technological tools and strategies that may help mitigate the insider threat. These technological approaches ranged from better authentication, and access control techniques to biometrics and application-based audit trails. The pros and cons of many of these approaches were debated.

Technologies in Use and Their Limitations

Authentication, access control, and audit trails are three well-understood technologies that can be used in combating the insider threat. Using these mechanisms to enforce strict accountability can be effective, but in practice they are often not as successful as

they might be. Participants agreed that understanding why this is the case⁴ and how to use available tools more effectively might be more useful than generating new research in these specific areas. Internal firewalls were also mentioned as a technique to achieve better protection against insider misuse.

Due to the vast amounts of data that are collected in audit logs it can be difficult to glean relevant information from them. However, even when not useful for on-the-fly analysis, audit logs, if properly created and secured, can be used as forensic evidence after the fact. Unfortunately, retaining large volumes of audit logs for long periods is quite expensive. Cost is always a factor. Participants pointed out that large amounts of money have been spent on *nuclear* security with good results. Risk management thus becomes a significant factor in deciding what amount of effort and resources to allocate to combating the insider threat. As another example, credit card companies go to great lengths to prevent and detect fraud. It was argued that the percentage of false positives (valid transactions deemed invalid) and false negatives (invalid transactions deemed valid)⁵ such companies will accept is much greater than that acceptable in some other domains (such as national security).

The mix of technologies that is employed in effecting information security deserves scrutiny. Questions that need to be asked include: What set of tools, technologies and strategies constitutes good security practice? Is there a widely accepted standard? If so, is it possible to reduce it to a set of business rules? If not, how could such a standard be developed? Participants identified a significant amount of technology that seems mature but whose application and/or implementation is less than optimal. The reasoning behind decisions about why and when such technology is deployed needs to be understood and communicated. Adding to the complexity, different security mechanisms are deployed in different environments. Often, strong security measures are not applied because the implementation is too difficult or is too user-unfriendly. Further examinations of how to better make use of available technology are needed. Distinguishing between best security practices and best *business* practices may prove useful in articulating the issues involved. Participants acknowledged the challenges in communicating technical security concerns to managers whose attention is often elsewhere.

Emerging Tools

There are a number of new research areas related to information security being explored. A list of potential research topics, some already underway include:

- Attack specification languages
- Intrusion Detection (signature-based, anomaly detection, object-based, distance measures, policy-based)
- New models of inside threat versus outside threat
- Authentication of roles, rights, privileges

⁴ Suggested reasons for the lack of success resulting from the use of current tools include difficulty of implementation, challenges to administration and maintenance, and poor management.

⁵ It was noted that credit card companies collectively lose on the order of \$1 billion per year and are willing to accept this amount of loss.

Meeting of November 1-2, 2000 on
Cyber-Security and the Insider Threat to Classified Information

- Semantics of authorized access
- Automated, dynamic revocation of privileges
- Profiling patterns of user behavior
- Response approaches (automated, recovery, reconstitution)
- Application-based intrusion detection
- Instrumentation of commercial off-the-shelf (COTS) applications
- Continuous biometrics
- Software for monitoring the system administrator
- Component verification
- Fingerprinting of documents
- Tagging technologies

A Rand workshop in August of 2000⁶ on the insider threat generated the following as the top research areas to which attention should be devoted in the next two to five years:

- Survivable architecture frameworks
- Differential access controls
- Provenance
- Mobile code (protect code from attack as well as systems from malicious code)

It was emphasized repeatedly that the insider threat and cyber-security problem is not merely a technological one. Good policies and policy enforcement are also necessary. Research is needed in how to define, describe, manage, and manipulate security policies. Systems can be abused through both bad policy and bad enforcement. Tools are needed to make setting and enforcing policy easier.

Another issue raised was the question of how to begin focusing security techniques at the application level, both centralized and distributed. Application-level audits to examine usage patterns (presuming that normal use of a particular application is well-defined) could be integrated with other kinds of audits to provide a more robust picture of system usage. In addition, a list of applications that are most often exploited by insiders could be used to provide guidance as to where attention should be focused. On the other hand, this runs the risk of an escalating ‘arms race’ as attackers become aware of the common knowledge and then focus their attentions elsewhere.

A particularly useful area of investigation would be to gain a more complete understanding of what sophisticated and successful system administrators do to protect their systems. Encapsulating that knowledge and codifying it somehow would provide insight into what the best kinds of defense are. Participants also noted that adding to system administrators’ security knowledge and overall resources would strengthen systems security.

Meeting participants emphasized that progress on this issue will be made only when researchers move beyond thinking about how to protect systems against relatively unsophisticated hackers and concentrate on how to protect against sophisticated, well-

⁶ The proceedings of this workshop are available at <http://www.rand.org/publications/CF/CF163/>.

financed attackers. If the costs of attacking a system can be made sufficiently high as to deter all but the most determined, then attention can be paid to the more difficult challenge presented by the truly skilled and motivated adversary (who in many case may well be an insider). Participants who have studied computer security over many years noted that, unfortunately, hacking information systems is becoming easier rather than more difficult. This is due to a number of factors, including the decline in the quality of COTS software, easily obtainable hacking toolsets and information, increased expertise in the general population, and poor default configurations that are not corrected by users.

5. Options for CSTB

A lively discussion took place about how a CSTB study in this area might best be oriented. As noted in the introduction, participants were nearly unanimous in their agreement that focusing exclusively on classified systems would not be appropriate. Several participants indicated that the Office of the Secretary of Defense (OSD) and the intelligence community can be (and likely already are) persuaded that this is a serious concern, and they would therefore be a good audience for such a study. However, limiting a study to classified networks and the classified aspects of information security would not produce as widely applicable a result as a broader conceptualization would. As has been described, corporations have very sensitive data and systems, and they invest in substantial protection just as the government does. Unclassified networks are often just as important (even in terms of national security) *and* just as likely to be attacked by a sophisticated adversary as are classified systems.

Participants argued that limiting such a project to classified systems would artificially constrain its sphere of influence. While acknowledging that much could be learned from a limited study that was, nonetheless, broadly applicable in the range of security issues it addressed, participants were concerned that such a limitation would also unnecessarily inhibit the size of the audience for such a report. The government currently uses COTS systems and any examination of such systems in a classified context will also likely produce useful results for those who use such systems in unclassified situations. More troubling is the possibility that a report focused only on classified systems (and the weaknesses in security thereof) could be used against the government were the report to lay out best practices that are not currently in place. CSTB has a history of examining governmental requirements versus commercial requirements and explicating the similarities and differences thereof, making a project of this scope feasible.

NEXT STEPS:

The participants in this meeting encouraged CSTB to develop a proposal for a study to examine high-grade threats (including insider threats) to high-value information systems. The study should focus both on national security concerns and classified systems as well as non-classified, commercial enterprises.

Meeting participants generated questions that such a study might address. They include, in no particular order:

- What is an appropriate characterization of ‘high-grade threat’ and ‘high-value target’?
- What are useful techniques to aid those who find themselves in charge of a high-value information system? What are good strategies to employ when a system is under attack by sophisticated adversaries (either self-motivated or organized and well-funded)?
- What is the extent to which insider and other serious threats are an unacknowledged or unreported issue within various communities?
- Is there information that should never be placed in electronic form?
- What is the responsibility of the industry when it comes to building secure systems and what role do recent laws such as the Uniform Computer Information Transactions Act (UCITA) and the Digital Millennium Copyright Act (DMCA) play?
- What are the sociological and managerial aspects of defending against high-grade threats?
- What data and what metrics are needed in order to begin modeling the problem of high-grade threats against high-grade targets?
- What are the upcoming technologies designed to help combat serious threats to high-value systems and what is their potential impact (e.g., what might be the future impact of quantum computing on these issues)?
- Given the new kinds of system and social organization becoming prevalent (e.g. peer-to-peer) are there changes in the security business model that need to be taken into account?
- Is software quality declining and therefore making the jobs of those likely to be attacked by serious, well-funded adversaries more difficult? If so, what can be done?

Appendix A

On The National Academies

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

The **Computer Science and Telecommunications Board (CSTB)** was established in 1986 to provide independent advice to the federal government on technical and public policy issues relating to computing and communications. Composed of leaders in the information technology and complementary fields from industry and academia, CSTB conducts studies of critical national issues that recommend actions or changes in actions by government, industry, academic researchers, and the larger nonprofit sector. CSTB also provides a neutral meeting ground for consideration and focusing of complex issues where resolution and action may be premature. It convenes invitational discussion sessions that bring together principals from the public and private sectors to share perspectives on all sides of an issue, assuring that the debate is not dominated by the loudest voices. Some of CSTB's recent work relevant to this meeting includes *Computers at Risk* (1991), *Continued Review of the Tax Systems Modernization of the Internal Revenue Service* (1995), *Trust in Cyberspace* (1999), and *Realizing the Potential of C4I* (2000).

Appendix B

**Planning Meeting on Cyber-Security and the Insider Threat to Classified
Information – November 1-2, 2000
List of Participants**

James Anderson

Independent Contractor

Edward Appel

Level 3 Communications

Mitchell Baxter

LegalNet Works Incorporated

Terry Benzel

Network Associates

Earl Boebert

Sandia National Laboratories

Thomas Bozek

Office of Secretary of Defense

Richard Brackney

National Security Agency

Michael Caloyannides

Mitretek Systems, Inc.

David "Beau" Davis

DISA/GC

John Davis

Mitretek Systems, Inc.

Anita Jones

University of Virginia

David Keene

Department of Defense

Terrence Kelly

White House Office of Science and
Technology Policy

Stephen Kent

BBN Technologies

Ronald Knecht

SAIC

Sandra Lambert

Lambert & Associates

Carl Landwehr

Mitretek Systems, Inc.

Karl Levitt

University of California, Davis

Gary McGraw

Cigital

Timothy Nagle

TRW

Robert Rosenthal

National Institute of Standards and
Technology

Roman Sloniewsky

Critical Infrastructure Assurance Office
U.S. Department of Commerce

Nicholas Trio

IBM T.J. Watson Research Center

Chenxi Wang

University of Virginia

Bradley Wood

SRI International

Michael Woods

Federal Bureau of Investigation

Bradley Woodworth

Pacific Northwest National Lab

Appendix C

Meeting Agenda

CYBER-SECURITY AND THE INSIDER THREAT TO CLASSIFIED INFORMATION

A PLANNING MEETING NOVEMBER 1-2, 2000

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD
NATIONAL RESEARCH COUNCIL
2001 WISCONSIN AVENUE, NW
GREEN BUILDING, ROOM 118
WASHINGTON, D.C.

Scope and Purpose:

The purpose of this exploratory meeting is to determine an appropriate role for the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) in examining information technologies (and related policy) to cope with "insider" threats to the cyber-security of classified information. Participants will examine the following inter-related topics: i) Are there issues with respect to the insider threat to classified systems that an NRC study could help address? If so, what are those issues? ii) How could CSTB help to identify and explicate a research agenda for information security technologies and associated policies and practices that are directed against the insider threat? iii) What would be the utility and impact of a CSTB study in this area?

If it is decided that a CSTB study would be useful, meeting participants will generate a set of questions that such a study should address. CSTB will subsequently develop a study proposal based on these questions. Sample questions/issues that such a study *might* address are included below to jump-start the discussion. Participants should feel free to disregard, expand upon, or otherwise change these sample questions. The goal is *not* to flesh out answers to these questions in detail, but to explore the surrounding issues enough to examine the nature and extent of the problem and to determine whether further investigation by an NRC-convened committee would be fruitful.

- What is an appropriate long-term technical research agenda that will address the issue of insider threat mitigation?
- What is the 'right' balance between technology and other strategies when attempting to prevent, detect, and respond to insider problems?
- Are there substantive distinctions between insider threats to classified and to unclassified systems and, if so, do such differences lend themselves to different technological strategies and/or policies?

For each of the interactive panels below, the panelists will each speak for 5-8 minutes to initiate discussion and the rest of the time will be spent in a roundtable discussion.

Meeting of November 1-2, 2000 on
Cyber-Security and the Insider Threat to Classified Information

Wednesday November 1, 2000

3:30 – 4:00pm **Welcome and overview of the NRC and CSTB**
Anita Jones, University of Virginia

4:00 – 5:30 **Panel: The Psychological and Social Aspects of the Insider Threat**
Michael Caloyannides, Mitretek Systems, Inc., [facilitator]
Bradley Wood, SRI International
David Keene, Defense Information Systems Agency

What are the psychological models of the insider? In what ways does the threat manifest itself for different types of insiders (e.g., disgruntled employees, blackmailed insiders, “sleepers”, unwitting accomplices, etc.)? Are there psychological and social issues that are more prevalent in military settings than in corporate settings? Does this change the nature of the strategies used against the insider threat? What policies and practices can actually be implemented that will help to cope effectively with the insider threat? Etc.

5:30 – 7:00 **Dinner with after dinner speaker**, Green Building, Room 126
A Management Framework for Security
Ron Knecht, Science Applications International Corporation

Thursday November 2, 2000

8:00 – 8:30am Breakfast

8:30 – 10:00 **Panel: State of the Practice – Technology**
Carl Landwehr, Mitretek Systems, Inc., [facilitator]
Nicholas Trio, IBM T. J. Watson Research Center
James Anderson, Consultant

What is the current state of the practice in terms of technological strategies to mitigate the insider threat? What technologies seem most effective? Which technologies are most commonly employed? Are these the most useful? Etc.

10:00 – 10:15 Break

10:15 – 11:45 **Panel: Emerging Capabilities and Future Research**
Karl Levitt, University of California, Davis [facilitator]
Earl Boebert, Sandia National Laboratories
Gary McGraw, Cigital
Terry Benzel, Network Associates

What are the open research questions with respect to the insider threat? Are there new technologies on the horizon that seem likely to be effective? What are the most vexing open problems, and why? Etc.

11:45 – 12:45 Lunch – **Case Studies: Legal Aspects of the Insider Threat to Information Systems**
Michael Woods, Federal Bureau of Investigation

Meeting of November 1-2, 2000 on
Cyber-Security and the Insider Threat to Classified Information

- 12:45 – 1:15 **Classified, Open, and Sensitive Systems**
Richard Brackney, National Security Agency
- 1:15 – 1:45 **Related NRC/CSTB Work: Topics for and Elements of a CSTB Project with Examples**
Marjory Blumenthal, Computer Science and Telecommunications Board
- 1:45 – 2:00 Break
- 2:00 – 4:00 **Roundtable discussion of what NRC/CSTB could do in this arena**
Anita Jones [facilitator]
- What are the major issues? What obstacles stand in the way of addressing them? Are there issues for which a consensus does not seem to have been reached in the community? Who is interested in addressing them? What benefits would be derived from solving them?
- Is a CSTB/NRC project on this subject warranted? If so, what questions should define the charge of the project? What parties might be interested in supporting such a project?
- 4:00 Adjourn