**THE PRESIDENTS**
**NATIONAL SECURITY TELECOMMUNICATIONS**
**ADVISORY COMMITTEE**


# PROTECTING SYSTEMS TASK FORCE REPORT ON ENHANCING THE NATION'S NETWORK SECURITY EFFORTS

## MAY 2000

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

## Background

Since early 1990, the United States Government and the President's National Security Telecommunications Advisory Committee (NSTAC) have been working together to address network security issues. NSTAC's efforts in this area have involved reviewing and conducting numerous studies regarding the risks to various infrastructures. Each risk assessment has reflected increasing awareness of the importance of network security and a corresponding but disproportionate increase in efforts to manage risk, address vulnerabilities, and deter the threat. The risk assessments have concluded that absent a valid baseline, there is little evidence to suggest that the risk has diminished and several factors to suggest that it is growing. Consequently, the NSTAC's Industry Executive Subcommittee (IES) established the Protecting Systems Task Force (PSTF) following NSTAC XXII and tasked it to—

> *Develop recommendations for the President regarding the focus of Government efforts to enhance the security of the Nation's telecommunications and information technology systems that support national security and emergency preparedness (NS/EP) activities.*

Risk has four basic aspects—***vulnerabilities***, mitigated by ***protection measures***, and ***threats***, mitigated by ***deterrents***—and each aspect influences overall risk. Vulnerabilities develop from continuing changes in products, processes, and business practices that are generally driven by technology development and market forces. Threats are composed of the motivation and capabilities of adversaries. Deterrents are driven primarily by law enforcement capabilities and priorities. Although those responsible for network security have very little, if any, control over these factors, they do have an opportunity to influence one aspect of risk–protection measures. Consequently, the PSTF decided to focus on this aspect of risk and the actions that can be taken to enhance network security by preventing, detecting, responding to, and mitigating intrusions.

## Objective and Methodology

The objective of this report is to examine current Government and industry network security strategies to determine whether alternative strategies might more effectively diminish risk and, if appropriate, make recommendations regarding those alternatives. The study focuses on those network security efforts intended to diminish the risks from unauthorized access to or activity in an information system and does not address physical security.

The PSTF based its study on information from the following sources:

- presentations from large, multinational telecommunications vendors and service providers with significant experience in network security,
- results of previous network security surveys,

- interviews with network security professionals,
- Government policy documents, white papers, reports, and briefings,
- presentations from network security conferences and forums, and
- previous research, including risk assessments.

The PSTF based its methodology for this study, in part, on a model of network security developed by the Intrusion Detection Subgroup (IDSG) of NSTAC's Network Group (NG) in 1997. The IDSG identified four basic components of network security:

- **Prevention.** Measures taken to preclude or deter an intrusion.
- **Detection.** Measures taken to identify that an intrusion has been attempted, is occurring, or has occurred.
- **Response.** An action or series of actions constituting a reply or reaction against an attempted or successful intrusion. Responses include actions taken to restore a network to its full operating capability following an attack.
- **Mitigation.** Actions taken to make the effects of an intrusion less severe. Mitigation actions include provision of alternative systems, system redundancy, and system fault tolerance.

Using this model, the PSTF sought to answer the following question:

> *Could the risk to network security be reduced more effectively by changing the relative focus of network security efforts among these four components?*

The PSTF's methodology involved five steps:

- **Current Focus.** Examine how Government and industry currently focus their efforts and allocate resources among the four network security components, in both operations and long-range initiatives.
- **Optimal Focus.** Determine how network security efforts should be optimally focused among the four components.
- **Changes Needed.** Determine what changes are needed to achieve the optimal focus of network security efforts among the four components (e.g., Government policies, legal issues, internal policies, management issues, technologies, corporate culture)
- **Barriers.** Identify barriers to those changes.
- **Government Actions.** Determine whether there are any actions the Government can take to address those barriers.

**Conclusions**

The ultimate question the PSTF sought to answer was:

> *Could shifting focus among the four components increase the overall level of network security, and, if so, what would the optimal focus be?*

At the outset, PSTF members expected the study would show that current Government efforts are focused too much on detection and the optimal approach would be a more balanced focus. The preliminary research—based largely on industry input—did not validate this expectation. There are a number of reasons for this:

- Each network is unique, with its own security requirements, so there is no "one-size-fits-all" approach to network security.
- The focus of efforts among the four elements *for any given network* may need to be restructured, or the focus may already be optimal.
- A shift in focus between today's approach and tomorrow's approach may not be driven by an inadequacy in the current approach. For example, perhaps today's priority is prevention and once that component has been addressed sufficiently, tomorrow's focus will be detection. In this case, each focus would be "optimal" for its particular situation. Alternatively, today's approach may be optimal for today's environment, and a new approach is required to achieve the optimal focus when the environment changes.
- Today's environment is dynamic. As described in Section 2.4, the Government has recently taken several actions to address network security issues (e.g., research and development (R&D) initiatives, security policy updates, acquisition guidance directives, and legislation), and these efforts will likely affect how the Government focuses its network security efforts.

For these reasons, the PSTF cannot recommend a particular focus of efforts among the four components that would apply to all networks. Although there is no ubiquitous optimal focus of network security efforts among the four components, it is essential that each organization develop *its own optimal focus* of network security efforts and policy based on the following factors:

- the organization's mission and the relative importance of factors such as availability, reliability, integrity, and confidentiality to that mission,
- the network's criticality to the organization's mission,
- the extent to which the network is connected to other networks, and
- the extent to which other networks depend on the network.

As a product of its research, the PSTF developed some *general observations* and compiled some *security policy principles*.

### *General Observations*

Although these general observations may not provide explicit guidance on how organizations might achieve the optimal focus of their network security efforts, they are factors an organization should consider in determining its approach to network security:

- Security is not a "one-size-fits-all" proposition.
- It is critical to focus on significant risk.
- There are limits to the scalability of incident response teams.
- Security should be considered an integral part of the enterprise architecture and in all stages of the system life cycle.
- Network security can be effective only if it is appropriately positioned within the organization, given sufficient prominence within the management structure, and resourced adequately.
- Security within an organization is multidimensional, and each dimension must be addressed appropriately.
- Incentives are needed to encourage implementation of effective but resource-intensive security guidelines.
- Regulations restricting technology transfer and export controls on encryption impede implementing security in global companies and services.
- Research and development should support an increased variety of products, tools, techniques, and practices to address all four network security components—prevention, detection, response, and mitigation, and their underlying security policy.

### *Security Policy Principles*

Security policy is an important factor in how organizations determine the focus of their network security efforts. Each entity indicated that security policies were not generally flexible enough to cope with changing architectural definitions of security, the dependence on commercial off-the-shelf products, and growing threat profiles. The following principles regarding security policy emerged from the PSTF's study:

- To ensure that security is not developed in a vacuum, organizations should incorporate security into their missions and create policies that meet the needs of the organization.

- The security measures required to implement those policies should not be considered as assets; instead, they should be considered as enablers to the organization's mission.
- Security policies should be risk based, not threat or vulnerability based.
- Although security policies cannot completely ignore technology, they should be technology neutral.
- Security policies should be enforceable.
- Security policies should be comprehensible and succinct.
- The board developing the policies within a company must be at a high level so that policies do not need to fight their way up the chain of command for approval.

**NSTAC Recommendation to the IES for Consideration in the NSTAC XXIV Work Plan**

While the PSTF gathered a representative sample of data to reflect a broad range of industry perspectives, the PSTF determined that it did not have sufficient information to adequately reflect the Government's perspective. Consequently, the PSTF decided to provide a status report to NSTAC XXIII in May 2000 and to propose the following:

> Based on the preliminary analysis and general observations of the Protecting Systems Task Force report, complete the analysis of the focus of network security efforts by seeking a broader range of input from Government and academia, as well as additional input from industry.

## 1.0 INTRODUCTION

This section provides the background for the study and sets forth the study's objective, approach, and methodology. In addition, it defines the terms used in the study and describes the document's organization.

### 1.1 Background

Since early 1990, the United States (U.S.) Government and the President's National Security Telecommunications Advisory Committee (NSTAC) have been working together to address network security issues. NSTAC's efforts in this area have involved reviewing and conducting several studies regarding the risks to various infrastructures. Each risk assessment has reflected increasing awareness of the importance of network security and a corresponding increase in efforts to protect against vulnerabilities and deter the threat. However, in spite of these efforts, all these risk assessments have reached similar conclusions: *Absent a valid baseline,... there is little evidence to suggest that the risk has diminished... and a number of factors to suggest that it is growing*.[1] Consequently, the NSTAC's Industry Executive Subcommittee (IES) established the Protecting Systems Task Force (PSTF) following NSTAC XXII in June 1999 and tasked it to—

> *Develop recommendations for the President regarding the focus of Government efforts to enhance the security of the Nation's telecommunications and information technology systems that support national security and emergency preparedness (NS/EP) activities.*

Risk has four basic—***vulnerabilities***, mitigated by ***protection measures***, and ***threats***, mitigated by ***deterrents***—and each aspect influences the overall risk. Vulnerabilities develop from continuing changes in products, processes, and business practices generally driven by technology development and market forces. Threats are composed of the motivation and capabilities of adversaries. Deterrents are driven primarily by law enforcement capabilities and priorities. Although those responsible for network security have very little, if any, control over these factors, they do have an opportunity to influence one aspect of risk—protection measures. Consequently, the PSTF decided to focus on this aspect of risk and the actions that can be taken to enhance network security by preventing, detecting, responding to, and mitigating intrusions.

### 1.2 Objective

The purpose of this report is to examine current Government and industry network security strategies to determine whether alternative strategies might more effectively diminish risk and, if appropriate, make recommendations regarding those alternatives. The study focuses on those

[1] *An Assessment of the Risk to the Security of the Public Network*, prepared by the U.S. Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIE), Office of the Manager, National Communications System, April 1999.

network security efforts intended to diminish the risk from unauthorized access to or activity in an information system and does not address physical security.

## 1.3 Approach

The study approach was to examine Government and industry network security practices using the following resources:

- presentations from large, multinational telecommunications vendors and service providers with significant experience in network security,
- results of previous network security surveys,
- interviews with network security professionals,
- Government policy documents, white papers, reports, and briefings,
- presentations from network security conferences and forums, and
- previous research, including risk assessments.

Appendix A provides a list of task force members, other participants, and contributing companies and Government agencies.

Because each of these information sources used a different network security taxonomy, the PSTF developed a common frame of reference to map the network security efforts of each data source to the four components. Appendix B, Components of Network Security and Their Indicators, provides a detailed description of the indicators associated with each component. The indicators serve two purposes:

- **Data gathering.** To map input from disparate sources to the four components as defined in this study.
- **Data analysis.** To facilitate analysis of the overall focus of operations and long-range initiatives.

## 1.4 Methodology

The PSTF based its methodology for this study, in part, on a model of network security developed by the Intrusion Detection Subgroup (IDSG) of NSTAC's Network Group (NG) in 1997.[2] The IDSG identified four basic components of network security: ***prevention***, ***detection***, ***response***, and ***mitigation***. Using this model, the PSTF sought to answer the following question:

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

*Could the risk to network security be more effectively reduced by changing the relative focus of network security efforts among these four components?*

The PSTF's methodology involved five steps as described below.

### *1.4.1 Current Focus*

In the first step, the PSTF examined how Government and industry currently focus their efforts and allocate resources among the four network security components, in both operations and long-range initiatives. The study of the focus of network security efforts among the components was not limited to current security operations but anticipated activities planned over the next few years. The methodology included identifying factors that could serve as indicators for each of the four components. (For example, one indicator of a *prevention* focus would be designating an individual to be responsible for ensuring the installation of security patches.) Each component has several indicators. (For a listing of each component and its indicators, refer to Appendix B, Components of Network Security and Their Indicators.) An organization's overall focus is determined by considering how the organization distributes its network security efforts among the four components.

### *1.4.2 Optimal Focus*

In the second step, the PSTF determined how network security efforts should optimally be focused among the four components.

### *1.4.3 Changes Needed*

In the third step, the PSTF determined what changes are needed to achieve the optimal focus of network security efforts among the four components (e.g., Government policies, legal issues, internal policies, management issues, technologies, corporate culture).

### *1.4.4 Barriers*

In the fourth step, the PSTF identified barriers to the changes identified in step 3.

### *1.4.5 Government Actions*

In the fifth and final step, the PSTF determined whether there are any actions the Government can take to address those barriers.

## 1.5 Terms

### *1.5.1 Network Security*

Network security is defined as the protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.[3]

### *1.5.2 Components of Network Security*

Although the components of network security defined below interrelate, for the purpose of discussion, they are considered to be discrete.

- **Prevention.** Measures taken to preclude or deter an intrusion.[4]
- **Detection.** Measures taken to identify that an intrusion has been attempted, is occurring, or has occurred.[5]
- **Response.** An action or series of actions constituting a reply or reaction against an attempted or successful intrusion. [6] Responses include actions taken to restore a network to its full operating capability following an attack.[7]
- **Mitigation.** Actions taken to make the effects of an intrusion less severe.[8] Mitigation actions include provision of alternative systems, system redundancy, and system fault tolerance. [9]

### *1.5.3 Intrusion*

Intrusion is defined as unauthorized access to, and activity in, an information system.[10] This broad definition includes unauthorized activities of both outsiders and insiders. Although insiders have authorized *access*, they may engage in *un*authorized *activities*, which are considered intrusions for the purpose of this report. For example, network management technicians have *authorized access* to routing tables, and they are *authorized* to engage in *defined activities*, such as rerouting traffic around congested nodes. However, they are *not*

[3] *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, January 1999, (Revision 1) [http://www.nstissc.gov/assets/pdf/4009.pdf].
[4] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[5] Ibid.
[6] Ibid.
[7] *Summary of Ongoing I&C CIP R&D Programs*, Information and Communications (I&C) Subgroup of the Critical Infrastructure Protection, Research and Development, and Interagency Working Group, May 26, 1999: Attachment A.
[8] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development.* op. cit.
[9] *Summary of Ongoing I&C CIP R&D Programs*, op. cit.
[10] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.

*authorized* to alter routing tables to *cause* congestion nor are they authorized to delete routing tables, and such acts would be considered intrusions. This expanded concept of intrusion is consistent with the definition of *intrusion* found in the 1999 version of the *National Security Agency Glossary of Terms in Security and Intrusion Detection:* "Any set of actions that attempts to compromise the integrity, confidentiality, or availability of a resource."[11]

## 1.6 Document Organization

The document is organized to follow the methodology described in Section 1.4. Section 2 describes the current focus; Section 3 describes the optimal strategy; Section 4 describes the barriers to optimal strategy; and Section 5 presents the conclusions.

[11] *NSA Glossary of Terms in Security and Intrusion Detection* [http://www.sans.org/newlook/resources/glossary.htm -- as of 8/27/99].

## 2.0 CURRENT FOCUS OF NETWORK SECURITY EFFORTS

This section addresses the current focus of network security efforts among the four network security components defined in Section 1.5.2, i.e., ***prevention***, ***detection***, ***response***, and ***mitigation***. For this study, "current focus" includes both what an organization is doing today and what long-range initiatives it is planning for the future. For example, even though an organization may have minimal intrusion detection systems (IDS) in place today, it may have long-range plans to substantially increase its use of IDSs. In combination, these factors indicate the extent to which the organization *currently* focuses its efforts on the detection component.

The overall depiction of the current focus of network security efforts set forth in this section is derived from information from both Government and industry sources. Government information includes Government policy documents, studies, white papers, and reports, as well as briefings to the PSTF from Government organizations responsible for addressing network security issues. Industry information includes briefings to the PSTF and interviews with network security professionals from telecommunications vendors and service providers. Network security surveys and material from network security conferences and forums provide additional information.

### 2.1 Survey of Operations

The respondents were asked to categorize their network security efforts by prevention, detection, response and mitigation. The PSTF asked respondents to indicate what percentage of their efforts were focused on each of these four components, using a combination of criteria such as budget, staffing levels, other resources, and general emphasis. Respondents were not asked to provide funding levels for each of the four components because accounting methods generally do not categorize expenditures in this way; even if these figures could be captured, they might be considered sensitive and proprietary. More importantly, however, the amount of money invested in information security is not necessarily the most accurate measure of an organization's focus on security, or even its level of security. Even if two organizations spend the same amount on security, one may achieve a substantially higher level of security than the other. One organization's spending may be minimal, and although it may secure only 50 percent of its systems, its implementation is correct because it focuses on the organization's most critical systems. Another organization may spend substantially more, securing 75 percent of its systems, but its implementation is inadequate because it does not focus on the most critical systems. In this case, the overall level of security of the first organization will be greater than that of the second.

#### *2.1.1 Government Perspectives*

The Government contributed to the overall NSTAC effort. In particular, the PSTF was briefed on network security initiatives of the Defense Department's Defense-wide Information Assurance Program (DIAP), as well as those of the Office of Management and Budget (OMB).

The DIAP is responsible for information assurance for the Department of Defense (DOD). DIAP's responsibilities include policy integration, security management, research and technology, critical infrastructure integration, monitoring the operational environment, incident response and acquisition support, and product development. These areas of responsibility address the network security components in various ways.

OMB is responsible for ensuring security policies are in place across agencies; the 2002 budget will require agencies to demonstrate to OMB that they understand the risks and costs associated with information security.[12] This requirement derives from the Paperwork Reduction Act of 1980, which assigned the Director of OMB responsibility for the following: 1) maintaining a comprehensive set of information resources management policies, and 2) promoting the application of information technology to improve the use and dissemination of information in the operation of Federal programs. *Office of Management and Budget (OMB) Circular A-130: Management of Federal Information Resources* provides this guidance and was revised in 1996 in response to the Paperwork Reduction Act of 1995.[13] In 1996, Appendix III of OMB Circular A-130 was issued to guide agencies in securing Government information resources as they continue to rely on an open and interconnected National Information Infrastructure by—

- providing a minimum set of controls to be included in Federal automated information security programs,
- assigning Federal agency responsibilities for the security of automated information, and
- linking agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123, Management Accountability and Control.[14]

Government contributions to the PSTF focused on higher level policy issues, and therefore could not be reflected in the percentages discussed in the following sections.

### *2.1.2 Survey Overview*

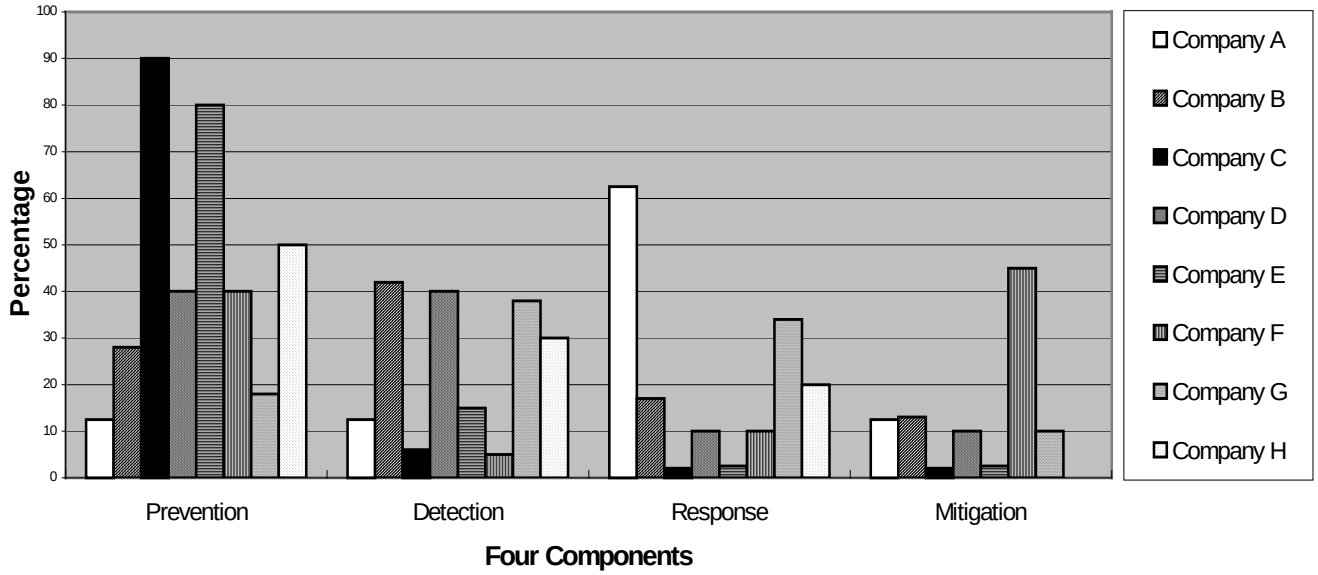
The survey revealed a wide array of disparate approaches to the focus of network security efforts among the four components. No unanimity exists because organizations implement security measures based on a number of considerations—their awareness, assessment, and tolerance of risk; their size, diversity, and level of maturity in network security; or their culture. However, analysis of the data does reflect a tendency to emphasize the first two components, prevention

[12] Memorandum for the Heads of Departments and Agencies, M-00-07, From: Jacob J. Lew, Director, Chief Information Officers Council, Subject: Incorporating and Funding Security in Information Systems Investments, February 28, 2000 [ http://www.cio.gov/docs/lews_lessons.htm].
[13] http://www.whitehouse.gov/omb/circulars/a130/a130.html.
[14] http://www.whitehouse.gov/omb/circulars/a123/a124.html.

and detection. For example, one company focuses heavily on prevention because it is trying to standardize security among its many acquisitions. After achieving certain goals, this company plans to reduce the emphasis on prevention and focus more heavily on detection. Additionally, because the company considers its mitigation and response components generally adequate, it does not plan to significantly increase its emphasis on those two components. Another company focuses heavily on response, which is necessary for the health of its business. However, this company would like to shift some of the efforts from the response component to the prevention component.

Figure 1 provides an overview of the responses of all the companies that described how they currently focus their network security efforts among the four components. Sections 2.1.3 through 2.1.6 and Figures 2 through 5 focus on each individual component.

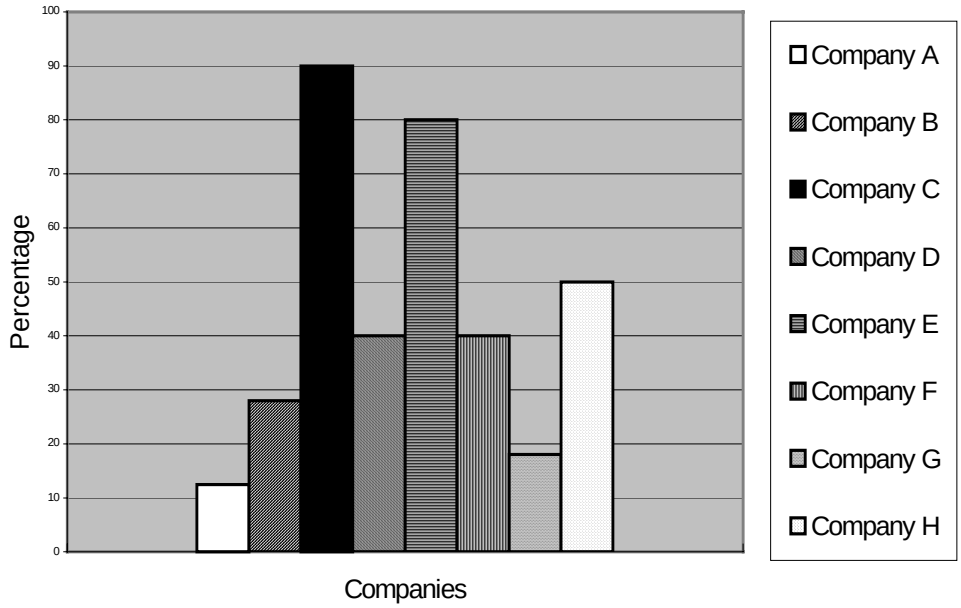
**Figure 1**
**Current Network Security Focus Across the Four Components**



### *2.1.3 Prevention*

Overall, network security efforts focused most heavily on the prevention component. The focus of efforts on prevention ranged from a low of 12.5 percent to a high of 90 percent (see Figure 2). The range reflects the companies' unique environments and the impact of those environments on their security requirements. Company A has minimal focus on prevention (only 12.5 percent) because most of its security efforts focus heavily on the response component, leaving few resources for prevention. At the other extreme, Company C dedicates 90 percent of its network security efforts to prevention because of the company's rapid and extensive growth.

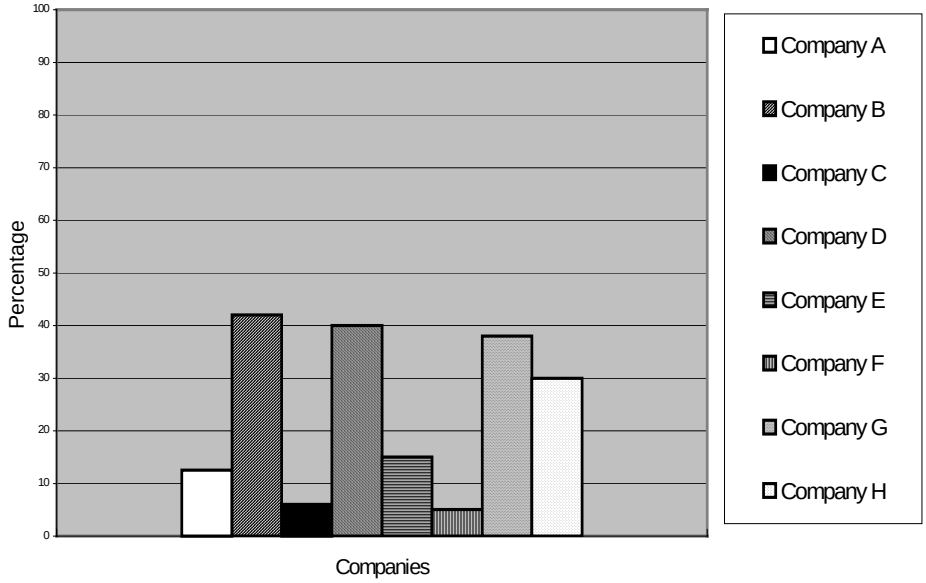
**Figure 2**
**Prevention Component**



### *2.1.4 Detection*

Responses from the companies surveyed show that focus on the detection component ranged from 5 percent to 42 percent (see Figure 3). Although companies generally reported a lower percentage of their focus on the detection component, this response does not indicate a lack of interest in detection. For example, Company A stated that the figure of 10 percent of its efforts focused on the detection component was misleading because the company uses automated tools, which are not very resource intensive. Most companies focused about 15 to 30 percent of their network security efforts on detection.

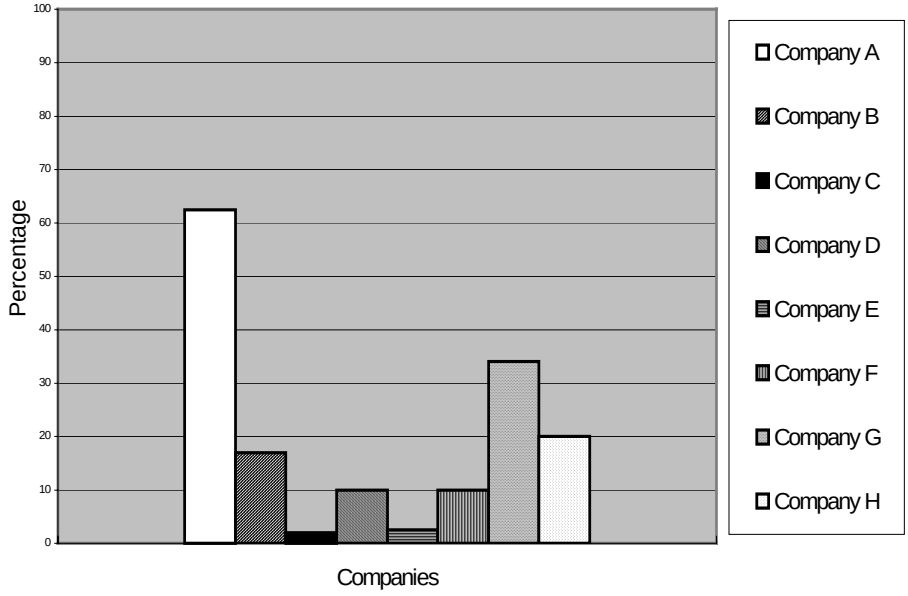
**Figure 3**
**Detection Component**



### *2.1.5 Response*

Allocation of network security efforts to the response component ranged from 2 percent to 62.5 percent (see Figure 4). For example, the nature of Company A's business requires the company to focus a majority of its network security efforts on response to incidents or inquiries about incidents. In contrast, Company E's approach is substantially different, choosing to respond to incidents only after they exceed a certain threshold. This latter approach minimizes the resources required for response. Most companies focused about 10 to 20 percent of their network security efforts on the response component.

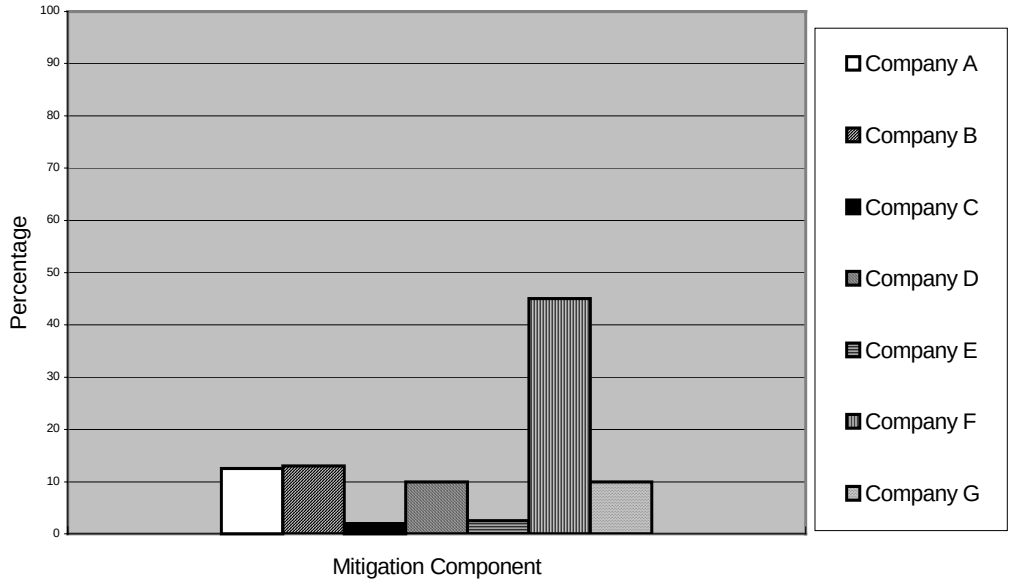
**Figure 4**
**Response Component**



### *2.1.6 Mitigation*

Generally, companies focused the least effort on the mitigation component. However, Company H reported that its allocation to the mitigation component was such a significant and integral part of its network security efforts that it could not provide a separate percentage on the mitigation component. Consequently, Figure 5 reflects mitigation allocations for only seven companies. Allocation of network security efforts to the mitigation component ranged from 2 to 45 percent. Mitigation is accomplished through system redundancy and backups. Most companies focus most heavily on the mitigation component when new systems or network components are incorporated into their infrastructure. The result is overall mitigation is low. Like Company H, Company F sees mitigation as an essential part of its network security practice, which is why its focus on mitigation is 45 percent. However, most companies focused only 10-13 percent of their network security efforts on mitigation.

**Figure 5**
**Mitigation Component**




## 2.2 Surveys of Computer Security Professionals

Computer industry surveys complemented the findings from the briefings and interviews. As expected, each survey used a slightly different taxonomy and framework to describe network security efforts. Nonetheless, the results can generally be mapped to the four components used in the PSTF's study. Although the PSTF's research included reviewing several surveys, the PSTF used the survey conducted by *Information Security Magazine* as a representative sample of

the others, because it was the most comprehensive and reflects the same basic results as the other surveys.[15]

Overall, security has gained increasing support over the past year. Each of the corporations surveyed had a security staff responsible for far more than just physical security. *Information Security Magazine* conducted a survey in April and May 1999 that was jointly sponsored by *ICSA TruSecure* and *Global Integrity Corporation*. The 1999 Industry Survey was completed by 745 qualified subscribers to the magazine. Respondents represented the best-informed and most security-conscious information technology (IT) professionals in Government and industry—administrators, managers, and executives with security, networking, and data management responsibilities. The goal of the survey was to assess the state of information security from the perspective of those responsible for it, pinpoint the obstacles to enterprise security, gauge the pervasiveness and effectiveness of commercial security products, and drill down into the increasing problems associated with security breaches.

On average, organizations' security budgets increased 21.7 percent from 1998 to 1999. In 1998, about 52 percent of the companies surveyed spent less than $50,000 on security; in 2000, it is projected only 38 percent will have security budgets that low. Responses to the *Information Security Magazine* survey indicated that the number of companies with security budgets exceeding $1 million is growing quickly. The number of companies with security budgets greater than $1 million a year was only 8 percent in 1999 but is projected to increase to 13 percent in 2000. Approximately 85 percent of all respondents said that security has improved at their organizations over the past 2 years. Although security overall has improved significantly, only 25 percent of respondents believed security staffing in their companies was adequate. The lack of adequate security staff, caused in part by the overall shortage of skilled security professionals in today's labor market, was also a common theme in responses provided to the PSTF from briefers and interviewees.

Of all the *Information Security Magazine* survey results, those related to product purchasing map most closely to the PSTF's network security components. Figure 6 reflects product purchasing trends. In 1998, 91 percent invested in virus protection (prevention), 90 percent in backup storage (mitigation), and 85 percent in access controls (prevention). In 1998, the respondents focused heavily on the prevention component, with an emphasis on virus protection; in 1999, the focus remained on prevention, but spending in this area shifted from virus protection to firewalls. In 1999, 82 percent of the respondents purchased firewalls, 77 percent invested in access controls, and 73 percent spent money on client/server security—all these measures fall on the prevention side of technology. At least 50 percent of the companies surveyed used products or services that fall into the prevention component, i.e., access control, encryption, firewalls, disaster recovery, and security for general e-mail, client/server applications, and network communications. Approximately 57 percent of the companies focused on disaster recovery, the response component. Only 41 percent had information security products or services related to

[15] *Information Security Magazine* 1999 Survey [ https://www.infosecuritymag.com/july99/].

intrusion detection; companies with larger security budgets were more inclined to invest in these tools. Companies with smaller budgets focused on access controls and firewalls (prevention).

**Figure 6**
**Product Purchasing Trends***

| 1998 | | 1999 | |
|---|---|---|---|
| **91 percent** | Virus Protection | **82 percent** | Firewalls |
| **90 percent** | Backup Storage | **77 percent** | Access Controls |
| **85 percent** | Access Controls | **73 percent** | Client/Server Security |
| **80 percent** | Physical Security | **67 percent** | LAN/WAN Security |
| **74 percent** | Firewalls | **59 percent** | Web Security |
| **73 percent** | Client/Server Security | **57 percent** | Disaster Recovery |
| **67 percent** | LAN/WAN Security | **57 percent** | Network/Communications Security |
| **61 percent** | Disaster Recovery | **56 percent** | E-Mail Security |
| **61 percent** | E-Mail Security | **50 percent** | Encryption |
| **60 percent** | Internet/Intranet/Web Security | **44 percent** | Mainframe Security |

***Source:** ***Information Security Magazine*** **1999 Survey**

Although spending on security has increased in terms of absolute dollars, GartnerGroup reported that, as a percentage of overall information technology costs, security expenditures remain relatively small. The GartnerGroup report showed that security expenditures accounted for only 2 percent of total desktop support costs and only 1 percent of remote access costs.[16]

## 2.3 Security Policy

Although security policy is not one of the four components, it clearly is a critical factor in how organizations focus their network security efforts. Each entity indicated that security policies were not generally flexible enough to cope with changing architectural definitions of security, the dependence on commercial off-the-shelf (COTS) products, and growing threat profiles. Respondents shared a number of ideas regarding the security policies that guide an organization's implementation of network security. These ideas are described in detail in Section 5.2, Security Policy Principles.

## 2.4 Emphasis of Long-Range Initiatives

There are a number of indications that Government and industry will be increasing the overall level of attention on network security:

[16] Peltier, Thomas, "Security Issues for 2000 and Beyond," presentation at 1999 Computer Security Institute Conference, November 15, 1999.

- Research and development (R&D) funds continue to increase across Government and industry. For example, in February 2000, President Clinton requested a 15 percent increase in funding for critical infrastructure protection for Fiscal Year 2000, inclusive of $606 million in funding for R&D, up from $451 million the previous year.[17]
- OMB is encouraging agencies to take greater responsibility for security. It has issued a policy update[18] regarding computer security policy and the budget process that mandates that Federal Government systems meet existing security criteria to receive continued funding and further states that no new funding will be granted for new projects until existing systems are compliant. This is not new policy but rather a refinement of existing Federal Government policies, such as those outlined in OMB Circular A-130 and the Computer Security Act of 1987. By tying the policies to the budget process, compliance can be enforced uniformly within the Government.
- In January 2000, the National Security Telecommunications Systems Security Committee (NSTISSC) issued *National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11*, "Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products." This policy applies to national security systems and ultimately will limit acquisition of COTS IA and IA-enabled IT products to those organizations that have been evaluated and validated in accordance with the International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement, the National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program, or the NIST Federal Information Processing Standard (FIPS) Validation Program.
- Some insurance companies are investigating network security as a requirement for insurance coverage, which could drive the private sector to invest more in security measures.
- The Congress is considering legislation to address information security issues (e.g., S. 1314/H.R. 2816, Computer Crime Enforcement Act; H.R. 850, Security and Freedom Through Encryption (SAFE) Act; S. 1756, National Laboratories Partnership Improvement Act of 1999, and S. 1993, Government Information Security Act of 1999).

Companies interviewed expect to refocus their network security efforts among the four components. Again, how they expect to shift their focus differs based on their goals, risks, and missions. One company expects its allocations to remain basically the same, based on the work it does. Currently, most of the work is focused on the response component, driven by the

[17] The White House, Office of the Press Secretary, "Cyber Security Initiatives," February 15, 2000.
[18] Memorandum for the Heads of Departments and Agencies, M-00-07, op. cit.

company's type of business; however, in the near future a small percentage of efforts focused on response will be reallocated to the prevention component. Another company expects to change its major emphasis from prevention to detection, with response and mitigation remaining constant.

Across the board, both Government and industry are planning to implement COTS products to meet their requirements. Intrusion detection tools are one of the most frequently mentioned type of COTS products. The greatest challenge with these tools is to diminish the number of false positive alerts and reduce the logs to a manageable size.

Respondents listed several other long-range initiatives:

- benchmarking networks,
- hiring good security personnel,
- implementing Public Key Infrastructure (PKI),
- improving user and management awareness, and
- improving internal security, because insiders are considered the greatest threat.

The *Information Security Magazine* survey offers further information on the direction of network security efforts (see Figures 7 and 8). Although intrusion detection was ranked only sixth in products and services currently in use (see Figure 7), it is at the top of the list of products companies plan to purchase in the next 12 months (see Figure 8). The other top purchases in the next 12 months are encryption, virtual private networks (VPN), and digital certificates. Remote access is an important issue in terms of security, with more employees working from home and traveling. The percentages allocated to VPNs and remote access security show that this issue is of great interest to many organizations. In addition, security vendors are working on products that offer single sign-on capabilities because companies want security to be simple so end users are more inclined to follow security policies and procedures rather than seek ways to work around onerous security measures. Biometric access controls are also growing in popularity because they can be far more convenient for users than passwords.

Figure 7 lists security products and services and the percentages of companies currently using them. Figure 8 lists security products and services and the percentage of companies planning to purchase them within the next 12 months. In both Figures, the security products and services are mapped to the four network security components using the PSTF's framework of security components and their indicators (see Appendix B).

**Figure 7**
**Security Products and Services Currently in Use***

| Products and Services | Network Security Components | Percent of Companies Currently Using Products and Services |
|---|---|---|
| Firewalls | Prevention | 82 |
| Access Controls | Prevention | 77 |
| Disaster Recovery | Response | 57 |
| Encryption | Prevention | 50 |
| Training/Education | Prevention | 42 |
| Intrusion Detection | Detection | 41 |
| Malicious Code Protection | Prevention | 38 |
| Digital Certificates | Prevention | 28 |
| VPN | Prevention | 27 |
| Smart Cards | Prevention | 19 |
| Single Sign-on | Prevention | 15 |
| PKI | Prevention | 14 |
| Biometrics | Prevention | 7 |

***Source: *Information Security Magazine* 1999 Survey**

**Figure 8**
**Security Products and Services Companies Plan to Purchase in the Next 12 Months***

| Products and Services | Network Security Components | Percent of Companies Planning to Purchase Products and Services |
|---|---|---|
| Intrusion Detection | Detection | 29 |
| Encryption | Prevention | 28 |
| VPN | Prevention | 28 |
| Digital Certificates | Prevention | 24 |
| Training/Education | Prevention | 23 |
| Firewalls | Prevention | 22 |
| PKI | Prevention | 21 |
| Single Sign-on | Prevention | 18 |
| Malicious Code Protection | Prevention | 18 |
| Disaster Recovery | Response | 17 |
| Smart Cards | Prevention | 17 |
| Access Controls | Prevention | 16 |
| Biometrics | Prevention | 11 |

***Source: *Information Security Magazine* 1999 Survey**

These findings are consistent with the comments provided by the companies that contributed to the PSTF's study directly—prevention seems to be an initial priority, and organizations begin to address detection only after achieving certain objectives in the prevention component.

## 2.5 Summary of Current Focus of Network Security Efforts

Government and industry organizations must determine how to focus their network security efforts among the four components based on their assessed risk, risk tolerance, company growth, stage of development, or culture. The briefings, interviews, and industry surveys show that although most organizations currently focus most heavily on prevention, this is expected to change as those factors influencing each organization's security strategy change, resulting in a shift to the other components. Across the board, prevention, and increasingly detection, have played the major role and will continue to do so.

As seen from the PSTF's findings and industry surveys, security is not a "one-size fits-all" proposition. Different systems or services have varying levels of acceptable risk. Further, each system or service has different needs for availability, confidentiality, and integrity.

## 3.0 OPTIMAL STRATEGY

While the previous section examines Government's and industry's depictions of the current focus of their network security efforts, this section addresses the views these sources have on what constitutes the optimal focus of network security efforts. It tackles the second step in the methodology described in Section 1.4, which is to determine how network security efforts should optimally be focused among the four components of prevention, detection, response, and mitigation. The purpose for doing so is to answer the following key question:

> *How can the Government best focus its network security efforts among the four components of prevention, detection, response, and mitigation to achieve optimal results?*

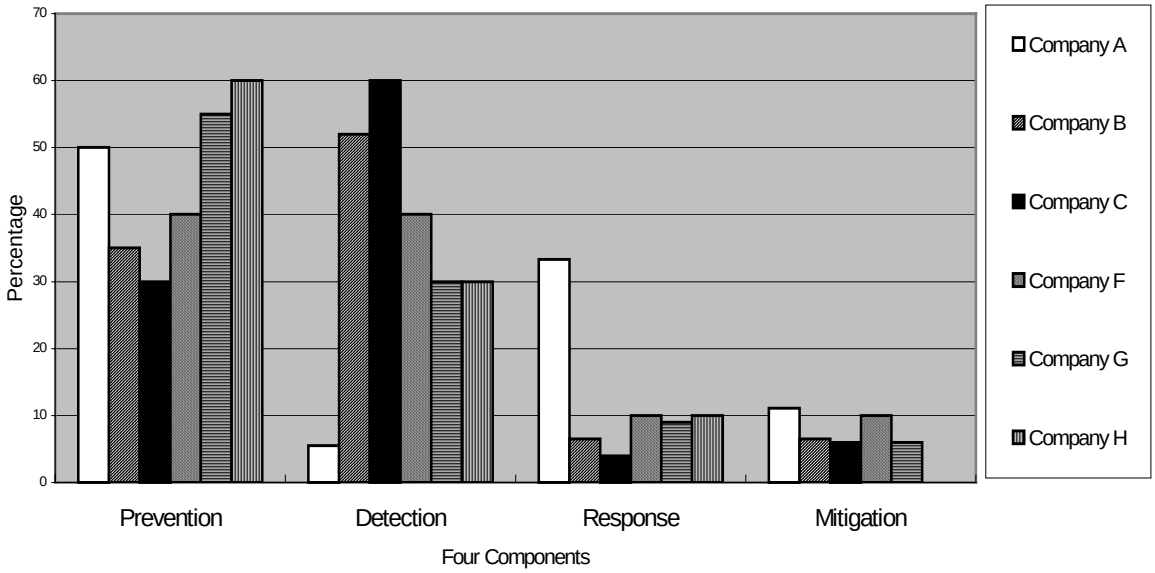
This appears to be a straightforward question that could easily be answered by researching the current and planned Government and industry efforts and identifying areas for improvement. However, the PSTF quickly discovered that answering this question was far more difficult than initially thought, for several reasons:

- Each company and Government organization queried was at a different level of experience and organizational maturity in network security. The level of experience and organizational maturity determined requirements, which led to priorities, budgets, resource allocation, and operational practices.
- Each organization's view of priorities also differed. In some cases, this view was a function of the extent of the organization's experience with network security operations; in other cases, it was simply a matter of preference. Although the various approaches to network security were unique to each organization, the PSTF identified several common themes, which will be discussed in greater detail below.
- Effective prioritization of components is not repeatable because the optimal solution for one organization may not be optimal for another.

### 3.1 Optimal Focus

Although there was great disparity among respondents on the recommended optimal focus of efforts among the four components, there were several common themes. Sections 3.1.1 through 3.1.4 summarize those themes, presented in order of the most often recommended to the least. Figure 9 provides an overview of the recommendations for optimal focus of efforts among the four components of network security. As was noted in Section 2.1.1, the results reflected in percentages were provided by industry because the Government contributions focused on higher level policy issues and consequently could not be reflected in percentages. Further, although eight companies responded with a breakdown of how they currently focus their network security efforts, only six provided percentages on their optimal focus.

**Figure 9**
**Optimal Focus of Network Security Efforts: Survey of Corporate Responses**




### *3.1.1 Prevention*

More information was offered regarding prevention than any other area. This area was most often cited as being in need of additional resources. The general view was that resources devoted to prevention would ultimately reduce the resources required for response and mitigation. Respondents addressed the following aspects of prevention:

- **Awareness.** An effective awareness campaign was viewed by more respondents than any other factor as the most critical to a successful network security program. Awareness includes all efforts to ensure employee, customer, and partner buy-in. A comprehensive cyber-ethics education program would contribute to the success of an awareness program.
- **Benchmarking.** Benchmarking was repeatedly viewed as more important than any single technology or practice. Based on risk and vulnerability assessments, benchmarking provides a data-centered starting point for improvements in network security.
- **Internet Protocol (IP) Security.** The next most important area for investment is the implementation of full IP Security (IPSec) for transport-mode privacy as an integrated part of a robust security architecture. Ideally, organizations should enable point-to-point encryption at multiple levels because corporate and organizational network perimeters can no longer be defined. With overlapping accesses granted to employees, contractors, suppliers, customers, and partners, trying to define and

defend a corporate perimeter no longer makes sense. Rather, identifying "islands" of security and implementing an encrypted VPN solution better address the security requirements of today's networking practices.

- **Public Key Infrastructure.** Almost as important as IPSec was a recommendation for robust PKI, including third-party authenticated certificate authorities.
- **Training.** To address the IT security skills gap, training and education programs were viewed as critical to the success of future networking. Although on-the-job training and internal classes are important elements of the overall training program, they should be augmented with more formal training leading to certification of security professionals.
- **Integration.** It was very important to respondents that security not be viewed as an "add-on" corrective measure. Rather than an add-on, security should be addressed as any other aspect or quality required to achieve the objectives of the enterprise. Funding for security should be provided not as a separate program, but in advance of all capital investments. Customer demand should generate market pressure on vendors to provide sufficient embedded security in all IT hardware and software products.
- **Standardized Reporting.** Standardized reporting mechanisms and communications protocols are needed to facilitate information sharing, rapid development of tools and procedures, and response, analysis, and mitigation processes.
- **Authentication.** Single sign-on schemes, possibly including biometric access controls, must replace the current reliance on reusable passwords and tokens for authentication. The goal should be to eliminate databases of passwords anywhere on corporate networks while providing more rigorous, user-friendly authentication.
- **IT Staff Authority**. The IT security staff must have executive visibility and authority to bring about meaningful change in corporate cultures.
- **Risk-Based Policies.** Security policies should be based on valid risk assessments, rather than on threats or vulnerabilities. Organizations must understand the levels of risk they are willing to accept and how that choice affects their implementation of network security measures. Also, security policy should become part of organizational mission statements.
- **Auditing.** Organizations should increase their auditing activities, both internal and third-party auditing. Auditing metrics also need to be further developed to maximize the utility of information gathered through audits.

### *3.1.2 Detection*

In recommending an optimal focus of efforts, respondents emphasized detection more than response or mitigation. Most often they discussed the need for a comprehensive, integrated

intrusion detection analysis capability. Centralized management of IDSs would greatly aid in this effort. Research and development is required to develop new IDS products, including a tool that can scan removable media. Efforts need to be made to eliminate false positive alerts and thereby reduce alarms to a manageable number, making more efficient use of the security staff. In addition, intrusion detection, network scanning, network analysis, visualization, and data reduction tools are becoming available and will help to identify and resolve problems and reduce logs to a manageable size. All these tools were viewed as extremely important, but they need improvement to become more operationally useful.

### *3.1.3 Response*

There was disagreement on whether additional resources should be devoted to response. While some companies recommended increases, others stated that increases in prevention would reduce the effort needed to respond to attacks, resulting in an overall gain in resource effectiveness and return on investment. Formalized incident response procedures, including measures of effectiveness, are required. Sharing information on lessons learned can lead to the development and adoption of best practices for response. Barriers to information sharing must be mitigated to allow for a truly robust incident response capability (see Section 4, Barriers).

### *3.1.4 Mitigation*

Redundancy was cited as important to mitigate the effects of outages and attacks, but current data storage capabilities are inadequate. The large volume of data required to manage networks is one aspect of data storage capability; another is the timeliness of the data, where losing as little as 5 minutes of updates and changes can be critical. A provisioning system to keep track of all data elements would greatly aid in categorizing and restoring network operations. Improved fault tolerance was also cited as an area needing additional effort.

## 3.2 Changes Needed

In addition to recommending an optimal focus of efforts, several companies identified issues that need to be addressed that could enhance the ability of Government and industry to pursue the network security strategy most effective for their individual organizations. These issues include incentives to encourage implementation of security guidelines, efforts to balance the interests of law enforcement with those of industry when responding to intruders, and changes needed to enable organizations to better manage their network security efforts.

### *3.2.1 Incentives*

Incentives are needed to encourage implementation of effective but resource-intensive security guidelines. Business decisions are based on the cost to implement security measures and weighed against the consequences of failure to implement them. One consideration is whether compliance offers the organization protection against liability. For example, insurance

companies require that jewelry stores remove jewelry from display windows after business hours. Meeting this requirement takes extra time, and prevents potential customers from window-shopping after hours. However, following this procedure protects the store owner from the liability of the loss in the event of a robbery. If the store fails to follow this procedure and a robbery occurs, the jewelry store owner would be liable for the loss; the insurance company would not reimburse the owner for this loss. By analogy, it might be useful to establish a level of due diligence such that if an organization follows certain guidelines, and despite these best efforts, the system is breached and someone is harmed, the organization would not be liable.

### *3.2.2 Law Enforcement Issues*

Currently, differences in law enforcement's goals and industry's goals may impede cooperation during an incident investigation. The goal of the law enforcement agency is to gather evidence that will help identify, apprehend, and successfully prosecute the criminal. The goal of the victim company is to diminish the damage and restore business operations as quickly, efficiently, and quietly as possible. It is sometimes difficult for both law enforcement and businesses to achieve their respective goals. Mutual understanding between law enforcement and business must be cultivated. Improved forensics tools that operate in the background could help.

### *3.2.3 Management Issues*

Education, metrics, and resources are management issues that must be addressed to improve the ability of organizations to more effectively focus their network security efforts.

- **Education.** Any efforts to accelerate workforce development would benefit Government and industry. Strong support was voiced for a national IT security education and training program.
- **Metrics.** Without metrics, neither Government nor the private sector can systematically improve network security. Metrics are required in many areas: personnel training, security state, and practices, among others. The Congress could spur the development of metrics by developing a grading system for Federal departments and agencies similar to that used during preparations for the Year 2000 rollover. [NOTE: Some concern was raised that the hacker community might use such information to identify which agencies are easier targets, but the Chief Information Officers (CIO) Council has subsequently drafted a grading system that takes this concern into account.] This is also an area for cooperation with the insurance and audit communities.
- **Resources.** Many organizations have limited resources to allocate to security measures and make their decisions on how to invest those limited resources based on their most recent security crisis. Such crisis-driven, reactive decision making does not result in the most effective use of an organization's resources. A better approach would be to proactively assess an organization's security needs and evaluate various

security measures to determine which ones will make the most effective use of limited funds.

### 3.3 Government Efforts

The Federal Government has already taken steps to improve network security. The DOD has the most mature program, but the non-DOD Federal Government is also addressing all the components expeditiously and logically. Consolidating oversight responsibility within OMB, organizing the CIO Council, and commissioning studies such as the National Defense Industrial Association (NDIA) study, *Computer Network Defense: An Industry Perspective*, have begun to demonstrate effective results in improving network security within Federal departments and agencies. Most of the network security work being done within the Federal Government focuses on defining a best-practices methodology. The NDIA study, the CIO Council's efforts, and others have begun to evaluate the many good ideas in Government, industry, and academia. This is not to say that the Federal Government's networks are secure, but that methodologies and structures now exist to enable the Government to adequately address the issues.

Whether risk could be reduced more effectively by changing the relative focus of network security efforts among the four basic components of prevention, detection, response, and mitigation is a valid question for individual departments, agencies, and programs. However, no single optimal focus is applicable to the entire Government. Moreover, the optimal focus of efforts for a single agency may not necessarily be optimal for another. Best practices, however, are generally applicable to Government and industry, across the board. How resources are allocated depends on several factors such as acceptable risk, level of security education and awareness, number of access points, and resources available.

### 3.4 Conclusion

Although no single solution is optimal for all network situations, it is critical that any organization consider the relative focus of network security efforts among the four components or any established taxonomy of network security technologies and actions. Establishing a baseline of an organization's security state, complemented with sound risk management, should form the basis for prioritizing network security efforts.

## 4.0 BARRIERS

Previous sections described the results of the PSTF's examination of Government's and industry's descriptions of the *current focus* of their network security efforts and their views on what constitutes the *optimal focus* of network security efforts. Because the current focus differs somewhat from the optimal focus, the PSTF sought to identify what factors might impede the implementation of those security measures that would result in the optimal focus. This section discusses factors considered barriers to the optimal focus of network security efforts.

Respondents offered varying perspectives on their security requirements and the factors limiting their ability to achieve the optimal focus of network security for their respective organizations. As noted in Section 3, Optimal Strategy, the PSTF discovered that the optimal solution for one organization may not be optimal for another. Consequently, a factor limiting one organization's ability to achieve its optimal focus may not affect another organization or may not affect it in the same way.

Barriers identified by respondents fall into four basic categories: ***technological***, ***cultural***, ***human factors***, and ***legal and regulatory***. The following sections describe these categories of barriers.

### 4.1 Technological Barriers

The sophistication of the threat and the ready availability of open source tools for adversaries has resulted in an acute awareness of the need to overcome technological barriers in the implementation, integration, and management of information security tools. Although several promising tools have been developed, the application of these products and the ease of implementation and management are still maturing. The development of the IPSec protocol as a standard for security communications and management will also enhance industry's ability to develop tools to manage heterogeneous environments. However, the goal of implementing an efficiently managed strategy of a distributed defense-in-depth that portrays a common picture of the operational health and security for the entire network is still not fully attainable.

The lack of the following technological capabilities was identified as limiting the ability of organizations to achieve an optimal strategy:

- an accepted monolithic security architecture that effectively implements a defense-in-depth concept,
- systems and software designed from the start to include security as a primary attribute rather than as an optional add-on,
- tools that present a manageable common picture portraying the operational health and security of an extended heterogeneous network architecture,
- scalability of management tools,

- easily integrated product suites that support the multitude of vendor products found in heterogeneous networks established over years of development,
- interoperability of vendor products including legacy systems and software,
- tools implementing mature artificial intelligence technology to eliminate false positive alerts and provide a predictive analysis capability,
- good, commercially available, data reduction tools,
- tools to facilitate response and mitigation (e.g., capabilities to back up the vast quantities of critical data that tend to be transitive in nature), and
- tools to facilitate information sharing and response, analysis, and mitigation processes.

Even when security tools are available, security personnel and administrators often are not adequately trained to use the tools provided or do not understand how to configure them correctly.

### 4.2 Cultural Barriers

An organization's culture has always been a major factor in determining how the organization approaches security. In today's interconnected environment, the security of one organization can be affected by the security of several other organizations. Previously, the security of a telecommunications service provider may not have been affected by a customer's approach to security; however, now providers give customers the capability to control their own services, and these customers have access to segments of the provider's systems. Consequently, the security of the provider's system can be affected by the level of a customer's security, as well as by the security level of any other entity with which that customer is interconnected (e.g., vendors, partners, customers). As a result, the organizational culture of one organization can affect the security of other organizations with which it is interconnected.

Organizational culture conflicts can arise between and within:

- market sectors/industries (e.g., telecommunications, manufacturing, agriculture, petroleum/chemical, garment),
- different companies in the same industry,
- corporate departments (e.g., marketing, production, financial, and information security),
- Government and industry organizations, and
- defense and civilian organizations.

Another factor that can drive cultural difference is the nature of the market; highly competitive national or international markets are more likely to have developed mechanisms to resolve cultural differences than less competitive niche, regional, and protected markets. More stable markets are also affected less by these barriers than markets that are still experiencing rapid growth.

One factor that can address the cultural barriers within organizations is the trend of establishing the role of the CIO at senior executive levels. Establishment of this formal, defined role has begun to achieve the level of visibility and emphasis needed for security to overcome many of these barriers, largely because it has become essential to maintaining competitiveness and corporate survivability. To some extent, the globalization of highly competitive, technology-dependent market sectors is resulting in identification of shared objectives with respect to security, which can help overcome the barriers caused by different organizational cultures. However, different countries, sectors, industries, companies, and departments will always have more or less unique cultures, and cultural differences will continue to limit organizations' effectiveness in developing strategies to implement security.

### 4.3 Human Factors Barriers

As with any endeavor, human factors play a significant role in achieving security objectives. People do not perform as expected or desired for a number of reasons:

- **Awareness.** They may not realize security is important.
- **Ability.** They may not know how to implement security.
- **Time.** They may have more work to do than available time permits.
- **Tools.** They may not have the tools they need.
- **Motivation.** There may be no consequences for failure to comply with security policies.
- **Malice.** They may have ulterior motives for not following security policies. For example, they may have a grudge against their employer or they may have something else to gain by violating security (e.g., selling proprietary information to competitors).

For the most part, these are management issues. Management is responsible for ensuring that employees are aware of security's importance and that they have the training, time, and tools to achieve expected security objectives. Management is also responsible for establishing individual performance requirements, clarifying the consequences for failure to meet those requirements, and taking disciplinary action when those requirements are not met. To some extent, removing some of the technological barriers described in Section 4.1 will have a positive effect on human factors by providing effective, easy-to-use security tools.

## 4.4 Legal and Regulatory Barriers

The legal and regulatory barriers to implementing an optimal security strategy identified by respondents fall into two general categories, export controls and information sharing. In addition, respondents identified regulatory lag as a concern. Technology evolves far more rapidly than legislation and regulation. When legislative and regulatory changes are needed to respond to technological issues, those changes may come too late to be effective.

### *4.4.1 Export Controls*

This category of barriers includes export controls on high-technology products and on encryption. Export restrictions may prevent companies with divisions or business partners located outside the United States from using certain products and the level of encryption they believe would best ensure the security of their operations. Another concern with encryption export controls is that U.S. vendors are reluctant to develop two versions of their products—one with encryption that can be used only within the United States, and one that can be exported—so they typically offer only products with exportable encryption. Because there are no restrictions on the level of encryption that can be imported, U.S. companies wanting higher levels of encryption buy such products from foreign vendors. This situation has economic implications for U.S. vendors and national security implications for the United States. The Government has recently taken actions to further relax export controls on encryption, but it is unclear what impact this might have.

### *4.4.2 Information Sharing*

The NSTAC has been addressing the information sharing issue since 1990, when its Network Security Task Force (NSTF) first identified the importance of sharing lessons learned regarding network security and recommended establishment of a mechanism to facilitate the exchange of network security information between the Government and NSTAC member companies. The NSTF's recommendation resulted in the establishment of the Government and NSTAC Network Security Information Exchanges (NSIE), which continue to share information regarding threats, vulnerabilities, and tools and techniques for addressing them.

With the advent of the Government's National Information Infrastructure initiative and the subsequent establishment of the President's Commission on Critical Infrastructure Protection (PCCIP), the information sharing issue continued to gather momentum. The NSTAC's Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force is addressing various aspects of this issue, and the NSTAC's Legislative and Regulatory Working Group (LRWG) is providing assistance with respect to the legal and regulatory issues affecting information sharing. Some of the legal and regulatory issues the industry participants identified as affecting information sharing included the following:

- **Freedom of Information Act (FOIA).** If a company shares information with the Government, there is the concern that once Government has this information, the company's competitors or the public could gain access to that information through a FOIA request. This concern makes companies reluctant to share such information with Government.
- **Antitrust Restrictions.** Companies may be willing to share information with a limited audience of trusted parties. However, because this approach would result in sharing information with some other companies and not others, the companies involved could run the risk of violating antitrust laws. Some companies may not believe that the advantages of sharing information outweigh the risk of violating antitrust laws, so they decline to share any information with any other company.
- **Liability.** Companies are concerned that disclosure of information about vulnerabilities or intrusion incidents may provide the grounds for liability claims against them, even if their customers were not actually harmed by these vulnerabilities or intrusion incidents. Consequently, companies are reluctant to share this kind of information.
- **Privacy Issues.** Although companies may want to screen potential employees, there are restrictions on how extensively they can check applicants' backgrounds. Hiring foreign nationals further complicates this issue.

These issues were also identified by the PCCIP as barriers to sharing information. These issues are beyond the scope of the PSTF's study.

## 5.0 CONCLUSIONS AND NSTAC DIRECTION TO THE IES

The ultimate question the PSTF sought to answer was—

> *Could shifting focus among the four components increase the overall level of network security, and, if so, what would the optimal focus be?*

At the outset, PSTF members expected the study would show that current Government efforts focus too much on detection and an optimal approach would be a more balanced focus. The preliminary research—based largely on industry input— did not validate this expectation. There are a number of reasons for this:

- Each network is unique, with its own security requirements, so there is no "one-size-fits-all" approach to network security.
- The focus of efforts among the four elements *for any given network* may need to be restructured, or the focus may already be optimal.
- A shift in focus between today's approach and tomorrow's approach may not be driven by an inadequacy in the current approach. For example, perhaps today's priority is prevention, and once that component has been sufficiently addressed, tomorrow's focus will be detection. In this case, each focus would be "optimal" for its particular situation. Alternatively, today's approach may be optimal for today's environment, and a new approach will be required to achieve the optimal focus when the environment changes.
- Today's environment is dynamic. As described in Section 2.4, the Government has recently take a number of actions to address network security issues (e.g., R&D initiatives, security policy updates, acquisition guidance directives, and legislation), and these efforts will likely affect how the Government focuses its network security efforts.

Although no ubiquitous optimal focus of network security efforts among the four components became clear after the industry study, several conclusions are significant. Each organization felt it must develop *its own optimal focus* of network security efforts. Rather than select a security approach or tool because another organization has found it useful or because of a persuasive magazine article, each organization must consider its own needs and focus its network security efforts among the four components to optimally meet those needs. An organization's security requirements will vary considerably, depending on the following factors:

- the organization's mission and the relative importance of factors such as availability, reliability, integrity, and confidentiality to that mission,
- the network's criticality to the organization's mission,

- the extent to which the network is connected to other networks, and
- the extent to which other networks depend on the network.

Rather than focus on security in a vacuum, organizations should consider security as one of the many factors associated with meeting its objectives and integrate security into its overall culture and architecture. First, the organization must determine its requirements for the assurance of availability, reliability, integrity, and confidentiality so it can maximize the effectiveness of its efforts to achieve those objectives. Once the organization determines its objectives in this area, then it must consider the factors that could affect the network's ability to meet those needs.

While the PSTF's analysis of preliminary data does not yield a recommendation for the Government to focus network security efforts among prevention, detection, response, and mitigation, the research resulted several useful observations. These observations are presented in Section 5.1.

In addition, as noted in Section 2, Current Focus, several principles regarding security policy emerged from the PSTF's study. These principles are delineated in Section 5.2. The PSTF's proposal for NSTAC direction to the IES is presented in Section 5.3.

## 5.1 General Observations

Although these general observations may not provide explicit guidance on how organizations might achieve the optimal focus of their network security efforts, they are factors an organization should consider in determining its approach to network security.

- **Security is not a "one-size-fits-all" proposition.** Different systems or services will have varying levels of acceptable risk. For example, a Web site that provides ZIP code information may have a lower tolerance for risk than a Web site that provides general organizational information about a Government agency. In responding to a natural disaster, it may be more important to have ZIP code information so emergency supplies can be shipped to the affected area than it is to know the organizational structure of the Federal Emergency Management Agency. Further, as discussed above, each system or service will have different needs for data integrity, availability, reliability, and confidentiality.
- **It is critical to focus on significant risk.** For example, attacks that merely deface Web sites are highly visible and often generate frenzied response. However, the problem is cosmetic, and the damage done to the Web page does not affect critical systems. Further, when the number of such attacks on Web sites is considered as a percentage of the total number of Web sites, it may be statistically insignificant. The level of resources and attention directed to responding to attacks that merely deface Web sites have no relation to the actual risk incurred. Resources should be directed

toward more critical issues, such as efforts to prevent denial of service attacks and theft or alteration of critical data.

- **There are limits to the scalability of incident response teams.** An organization's incident response practices must accommodate its products, services, size, diversity, and topography. As an organization grows, it may require different incident response teams focused on different aspects of its networks.
- **Security should be considered an integral part of the enterprise architecture and in all stages of the system life cycle.** In designing a system or service, criteria such as acceptable levels of availability (e.g., 99.99 percent), integrity (e.g., bit error rate of .001 percent), and reliability (e.g., delivery within three business days), are considered, and the architecture is designed to meet those criteria. Rather than an add-on, security should be addressed as any other aspect or quality required to achieve the objectives of the enterprise.
- **Network security can be effective only if it is appropriately positioned within the organization, given sufficient prominence within the management structure, and resourced adequately.** Achieving this objective is directly related to management support, availability of training, and the extent to which available tools are deployed.
  - **Management.** Network security must be prominently positioned within the organization to demonstrate upper management's support and ensure adequate visibility and emphasis within the organization.
  - **Training.** Training is a key aspect of security. Training budgets should include funds for security training; IT professionals should be cross-trained in all aspects of security. Often security tools are not being used correctly because of inadequate training, which precludes achieving the maximum return on the organization's investment in those tools.
  - **Tools.** Although better security tools are undoubtedly needed, organizations may not take full advantage of the tools already available because it is difficult to keep up with the latest product developments. Other factors include the cost of the tools and lack of skilled staff to use them.
- **Security within an organization is multidimensional, and each dimension must be addressed appropriately.** Not all systems are critical, and not all aspects of critical systems have the same degree of criticality. Criticalities should be defined and resources should be allocated accordingly.
- **Incentives are needed to encourage implementation of effective but resource-intensive security guidelines.** Business decisions are based on the cost to implement security measures and weighed against the impact of failure to implement them. As discussed in Section 3.2.1, one consideration is whether compliance will offer the organization protection against liability.

- **Regulations restricting technology transfer and export controls on encryption impede implementing security in global companies and services.** Export controls have economic implications for U.S. vendors and national security implications for the United States. The Government has recently taken action to further relax export controls on encryption, but it is unclear what impact this might have.
- **Research and development should support an increased variety of products, tools, techniques, and practices to address all four network security components—prevention, detection, response, and mitigation—and their underlying security policy.** Desired technologies include data reduction and automated response and mitigation.

## 5.2 Security Policy Principles

As noted in Section 2.3, security policy is an important factor in how organizations determine the focus of their network security efforts. This section briefly describes a few principles regarding security policy that emerged from the PSTF's study.

- **To ensure that security is not developed in a vacuum, organizations should incorporate security into their missions and create policies that meet the needs of the organization.** A key factor to consider when developing security policies is that program officials, not security officers, will be responsible for implementation. Consequently, policies should take into account the organization's mission and functional requirements so that the program officials will see how the security policy supports the program's mission and why it is important to implement such policies. It is also essential to obtain user buy-in on security policies.
- **The security measures required to implement those policies should not be considered as assets; instead, they should be considered as enablers to the organization's mission.** If security investments are viewed as assets, they will likely show a low return on investment and consequently may be perceived as a drain on the budget. If viewed as enablers, investments in security will be recognized as essential elements for fulfilling the organization's mission.
- **Security policies should be risk based, not threat or vulnerability based.** They should take into account both the level of risk acceptable to the program and the cost-effectiveness of security measures intended to achieve the level of protection required.
- **Although security policies cannot completely ignore technology, they should be technology neutral.** One company had general security policies, complemented by technology-specific security procedures. When the technology was retired, the general security policies were still applicable, even though technology-specific procedures were retired.

- **Security policies should be enforceable.** Security policies should be written with organizational constraints in mind; otherwise, they cannot be enforced. For example, security policies should take budget constraints into consideration so that security policies will be enforceable and can be supported by available resources.
- **Security policies should be comprehensible and succinct.** Users are unlikely to follow policies unless they are easy to understand and remember.
- **The board developing the policies within a company must be at a high level so that policies do not need to fight their way up the chain of command for approval.** A board of high-level managers will have the authority to approve policies quickly.

## 5.3 NSTAC Recommendation to the IES for Consideration in the NSTAC XXIV Work Plan

While the PSTF gathered a representative sample of data to reflect a broad range of industry perspectives, the PSTF determined that it did not have sufficient information to adequately reflect the Government's perspective. Consequently, the PSTF decided to provide a status report to NSTAC XXIII in May 2000 and to propose the following:

> Based on the preliminary analysis and general observations of the Protecting Systems Task Force report, complete the analysis of the focus of network security efforts by seeking a broader range of input from Government and academia, as well as additional input from industry.

# APPENDIX A

# TASK FORCE MEMBERS AND OTHER CONTRIBUTORS

## TASK FORCE MEMBERS

| | |
|---|---|
| Cisco Systems | Mr. Ken Watson, Chair |
| NTA | Mr. Bob Burns, Vice Chair |
| AT&T | Mr. Paul Waldner |
| Boeing | Mr. Bob Steele |
| CSC | Mr. Guy Copeland |
| EDS | Mr. Randy Jensen |
| GTE | Mr. James Bean |
| ITT | Mr. Dave Kelly |
| Lockheed Martin | Dr. Chris Feudo |
| MCI WorldCom | Mr. Mike McPadden |
| Nortel Networks | Dr. Jack Edwards |
| Raytheon | Mr. Thomas O'Connell |
| SAIC | Mr. Nelson Williams, Jr. |
| U S WEST | Mr. Jon Lofstedt |

## OTHER PARTICIPANTS

| | |
|---|---|
| AT&T | Mr. Harry Underhill |
| Cisco Systems | Mr. Jim Massa |
| COMSAT | Dr. Jack Oslund<br>Mr. David Roberson |
| GTE | Ms. Ernie Gormsen<br>Mr. Lowell Thomas |
| ITT | Mr. Joe Gancie<br>Dr. Stuart Cohen |
| NTA | Mr. Shawn Cochran |
| SAIC | Mr. Hank Kluepfel |

## COMPANY/AGENCY CONTRIBUTORS

AT&T

Bell South

Cisco Systems

COMSAT

CSC

Department of Defense—Defense-wide Information Assurance Program

GTE

ITT

Lockheed Martin

Department of Commerce—National Telecommunications and Information Administration

Department of Commerce—National Institute of Standards and Technology

Executive Office of the President—Office of Management and Budget

Raytheon

Rockwell

SAIC

# APPENDIX B

# COMPONENTS OF NETWORK SECURITY AND THEIR INDICATORS

## COMPONENTS OF NETWORK SECURITY AND THEIR INDICATORS

### PURPOSE OF THIS DOCUMENT

This document sets forth the categories and definitions of the components of network security that the Protecting Systems Task Force (PSTF) of the President's National Security Telecommunications Advisory Committee (NSTAC) has selected to frame its work to address its tasking:

> Develop recommendations for the President regarding the focus of Government efforts to enhance the security of the Nation's telecommunications and information technology systems that support national security and emergency preparedness (NS/EP) activities.

The PSTF recognizes that there are several valid approaches to categorizing and defining the components of network security. The PSTF has selected one such approach and has developed this document to enable subject matter experts with varied perspectives to map their respective inputs to a common framework.

Because the PSTF is tasked to make recommendations regarding the focus of Government efforts, we ask that you take into account the following additional areas when formulating your response:

- Consider what percentage of your organization's total information technology (IT) budget is allocated to IT security personnel, IT security time, and IT security budget.
- Identify which initiatives are most effective, least effective, have the most favorable cost/benefit ratio, and are essential regardless of cost.
- Consider how Government policies and practices benefit you, hinder you, or may be changed. Also consider what new or revised Government initiatives would be most helpful.

For purposes of the PSTF's report, network security is composed of four components, listed and defined below:

- **Prevention**: Measures to preclude or deter an intrusion.
- **Detection:** Measures taken to identify that an intrusion has been attempted, is occurring, or has occurred.
- **Response:** An action or series of actions constituting a reply or reaction against an attempted or successful intrusion. Includes actions taken to restore a network to its full operating capability following an attack.

- **Mitigation:** Actions taken to make the effects of an intrusion less severe. Mitigation actions include provision of alternative systems, system redundancy, and system fault tolerance.

Because "intrusion" is a key term used to define the components, its definition for the purposes of the PSTF report will be:

- **Intrusion:** Any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource.

The PSTF also recognizes that some actions or conditions could reasonably be considered indicators of more than one component. Consequently, the PSTF also describes how, for the purpose of this report, the indicators map to each component. It is hoped that this common framework will facilitate data gathering and analysis for this study.

## SECURITY POLICY/PLAN

Network security efforts focus on four basic components: *prevention, detection, response* and *mitigation*. For these components to be effective, security policies, procedures and plans must be defined that span all four components.

Indicators relating to security policies and plans are listed below. Because policies and plans are established at the upper management level and apply to all four components, they are addressed separately. Indicators related to each of the four components of network security follow.

### Definition

> *The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.*[1]

### The following conditions are indicators of efforts focused on security policies and plans.

**1. Security Policy**

- 1.1. The organization has an established security policy.
  - 1.1.1. The security policy is routinely reviewed and updated.
  - 1.1.2. The security policy establishes standards for how information systems should be configured and operated.
- 1.2. The security policy addresses configuration management/change control.
- 1.3. The security policy addresses disaster recovery.
- 1.4. The security policy addresses data protection.
- 1.5. The security policy addresses interoperability.
- 1.6. The security policy addresses physical access to critical components, including:
  - 1.6.1. Established policies for lock/key changes when employees/contractors are re-assigned or leave.
  - 1.6.2. Policies governing moving equipment from the premises.
- 1.7. The organization has established codes of conduct.
- 1.8. Security is made visible in the organization.
- 1.9. Compliance with security policy is monitored.
- 1.10. The organization performs risk assessment or security business impact analysis studies.
- 1.11. Risk assessments or business impact analyses are performed before installation of new hardware, operating systems, and significant changes.

[1] *NSA Glossary of Terms in Security and Intrusion Detection*, 1998, *[*http://www.sans.org/newlook/resources/glossary.htm *– as of 8/27/99]*

**2. Security Plan**

2.1. The organization uses the System Security Engineering Capability Maturity Model (SSE-CMM) to incorporate security into systems when they are built.

2.1.1. The model has metrics by which the level of security of your system can be measured or rated.

2.2. Security personnel are involved in the planning process for implementing cost-saving changes.

2.3. A security plan exists for each system.

2.3.1. The uses of each system are explicitly defined.

2.3.2. Each system runs only those services that support its uses. Unnecessary services are disabled (e.g., *sendmail*, *rpc*, *statd* on a public Web site).

2.3.3. Each system has a documented baseline.

2.4. The uses of each network are explicitly defined.

2.4.1. Unnecessary or unauthorized protocols for each network are disabled.

2.4.2. Each network has a documented baseline.

**3. Security Metrics**

3.1. The organization has established security metrics.

## COMPONENT 1: PREVENTION

### Definition

*Measures taken to preclude or deter an intrusion.*[2]

**The following conditions are indicators of efforts focused on prevention.**

1. **Access Control**
   - 1.1. The organization has established criteria for assigning logins, passwords, privileges/rights, login expirations, account lock-outs.
   - 1.2. Separation of functions are enforced using role-based access or other mechanisms for enforcing granular access.
   - 1.3. The organization has established procedures or automatic mechanisms for deactivating user logins when employees/contractors are re-assigned or leave.

2. **Authentication**
   - 2.1. Authentication is used (e.g., passwords, one-time passwords, token-based, biometrics).
     - 2.1.1. The organization has standards for users to follow to ensure they select secure passwords.
   - 2.2. The organization supports digital signatures and ensures their security.

3. **Confidentiality**
   - 3.1. Sensitive data is encrypted
     - 3.1.1. At the file level
     - 3.1.2. At the transmission level

4. **Interoperability**
   - 4.1. Compliance tests or independent validation and verification (IV&V) actions are implemented to help ensure interoperability across various platforms and vendor releases.

5. **Integrity**
   - 5.1. Integrity checks are conducted to ensure that data was not modified in transmission.

[2] *Network Group Intrusion Detection Subgroup: Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, The President's National Security Telecommunications Advisory Committee, December 1997.

**6. Vulnerabilities**

6.1. There is an organization wide effort to identify vulnerabilities.
6.2. Vulnerability scans are run on a routine basis.
  6.2.1. Multiple scans are run.
  6.2.2. Results are correlated.
6.3. System administrators are supported in correcting vulnerabilities.
6.4. There is an established procedure for obtaining fixes and installing them.
  6.4.1. Installations of patches for known vulnerabilities are verified.
  6.4.2. Security suggestions published by the vendors are implemented.
6.5. Metrics are in place to determine the effectiveness of efforts to remove vulnerabilities.
6.6. There is a corporate anti-virus program.
  6.6.1. It includes signatures for known Trojan horse programs.
  6.6.2. There are set procedures for updates/upgrades.
  6.6.3. There are established response procedures for new virus alerts, like the Melissa virus.
  6.6.4. Virus scanning is conducted at multiple levels (e.g., desktop, server, mail gateway).

**7. Training/Awareness**

7.1. There is an education and awareness program.
7.2. Training programs are formalized to ensure consistent training throughout the organization.
7.3. System administrators are trained on security.
7.4. There is a certification program for system administrators and security administrators.
7.5. End-users are trained on security.
7.6. The level of training is sufficient to ensure that personnel can follow security policies, identify security problems, and implement solutions.
7.7. The organization keeps up with what "bad people" are doing and alerts system administrators and end-users of potential threats.

**8. Management**

8.1. The organization has dedicated network staff and backup staff.
8.2. Individuals are responsible for only the *number* of components they can effectively manage.
8.3. Individuals are responsible for only the *types* of components they can understand.
8.4. There are adequate checks and balances to ensure that one individual does not have excessive power/access.

**9. Internet Interconnections**

9.1. Security between internal systems and the Internet is addressed.
9.2. The organization uses firewalls.
9.3. The organization uses virtual private networks (VPN).
9.4. The organization monitors Internet connectivity for unauthorized access.

## COMPONENT 2: DETECTION

### Definition

*Measures taken to identify that an intrusion has been attempted, is occurring, or has occurred.* [3]

**The following conditions are indicators of efforts focused on detection.**

1. **Audit Logs**
   - 1.1. Audit logging is required and implemented on all information technology systems.
   - 1.2. The logs are stored in secure locations.
   - 1.3. Audit logs are reviewed regularly for unusual or suspicious activity.
     - 1.3.1. The review is conducted manually or automated and based on user or signature profiles.

2. **Intrusion Detection**
   - 2.1. The organization has a strategy to determine that something is wrong in the network.
   - 2.2. The organization uses an intrusion detection tool.
   - 2.3. The organization uses more than one intrusion detection tool.
     - 2.3.1. The organization determines which intrusion detection tool(s) to use on which system(s) by assessing the criticality of each system, using more robust (or more layers of) intrusion detection tools on the most critical systems and data.
     - 2.3.2. The organization correlates intrusion data from multiple intrusion detection tools, or from multiple systems.
   - 2.4. Host-based intrusion detection systems are deployed.
   - 2.5. Network-based intrusion detection systems are deployed.
   - 2.6. "Honeypots" are used to divert intrusions.
   - 2.7. The organization has established mechanism for reporting intrusion incidents.

[3] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.

## COMPONENT 3: RESPONSE

### Definition

*An action or series of actions constituting a reply or reaction against an attempted or successful intrusion.*[4] *Includes actions taken to restore a network to its full operating capability following an attack.*[5]

**The following conditions are indicators of efforts focused on response.**

**1. Recovery/Restoration**

1.1. The organization has a disaster recovery plan.
1.2. The disaster recovery plan addresses recovery from security incidents.
1.3. The plan is stored in a secure, accessible place.
1.4. The disaster recovery plan is tested periodically.

**2. Incident Response**

2.1. There is a team in place responsible for handling *major* security incidents.
2.2. There is a team in place responsible for handling *day-to-day* incidents.
2.3. The organization has established response procedures.
2.4. The organization maintains a list of contacts to notify of suspected intrusions and routinely updates that list.
2.5. The organization has established a policy on reporting incidents to law enforcement.
  2.5.1. There are established procedures for protecting the chain of evidence to meet requirements for prosecution.
  2.5.2. Personnel are trained on these procedures.

[4] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[5] *Summary of Ongoing I&C CIP R&D Programs.* Information and Communications (I&C) Subgroup of the Critical Infrastructure Protection, Research and Development, and Interagency Working Group, May 26, 1999: Attachment A.

## COMPONENT 4: MITIGATION

### Definition

*Actions taken to make the effects of an intrusion less severe. [6]Mitigation actions include provision of alternative systems, system redundancy, and system fault tolerance.[7]*

**The following conditions are indicators of efforts focused on response.**

1. **Redundancy/Diversity/Fault Tolerance**
   - 1.1. Critical systems have redundancy.
   - 1.2. In the event of significant failures, the organization has: a hot site standing by, a cold site, and/or server replications.
   - 1.3. The hot site, cold site, and/or server replications have been tested.
   - 1.4. Critical systems have diversity.
   - 1.5. Critical systems employ fault tolerant mechanisms.

2. **Backups**
   - 2.1. The organization has established back-up procedures.
     - 2.1.1. Data backups are maintained.
     - 2.1.2. System backups are maintained.
     - 2.1.3. Critical data and systems are backed up with a frequency consistent with their criticality.
   - 2.2. Back-up media is routinely stored on site.
   - 2.3. Back-up media is routinely stored off site.
   - 2.4. Workstations are routinely backed up. End-users are instructed on how to back up their critical data.
   - 2.5. Business records (accounting, human resources, etc.) are archived with a frequency consistent with their criticality.

3. **Interfaces**
   - 3.1. Systems interfaces are documented and well-understood.
   - 3.2. Systems administrators and security staff are cognizant of the extent to which a successful intrusion into one system will allow the intruder to access any other systems.
   - 3.3. Mitigation procedures effectively preclude failure in one system from causing failures to other systems with which they interface.

[6] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[7] *Summary of Ongoing I&C CIP R&D Programs*, op. cit.

# APPENDIX C

# ACRONYM LIST

# ACRONYMS

| | |
|---|---|
| CIO | Chief Information Officer |
| COTS | Commercial Off-the-Shelf |
| DIAP | Defense-wide Information Assurance Program |
| DOD | Department of Defense |
| FIPS | Federal Information Processing Standard |
| FOIA | Freedom of Information Act |
| GAO | General Accounting Office |
| I&C | Information and Communications |
| IA | Information Assurance |
| IDS | Intrusion Detection Systems |
| IDSG | Intrusion Detection Subgroup |
| IEPS | International Emergency Preference Scheme |
| IES | Industry Executive Subcommittee |
| INFOSEC | Information Security |
| IP | Internet Protocol |
| IPSec | Internet Protocol Security |
| IS/CIP | Information Sharing/Critical Infrastructure Protection Task Force |
| IT | Information Technology |
| IV&V | Independent Validation and Verification |
| LAN | Local Area Network |
| LRWG | Legislative and Regulatory Working Group |
| NCS | National Communications System |
| NDIA | National Defense Industrial Association |
| NG | Network Group |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NS/EP | National Security Emergency Preparedness |

| | |
|---|---|
| NSIE | Network Security Information Exchange |
| NSTAC | National Security Telecommunications Advisory Committee |
| NSTISSC | National Security Telecommunications and Information Systems Security Committee |
| NSTISSP | National Security Telecommunications and Information Systems Security Policy |
| NSTF | Network Security Task Force |
| OMB | Office of Management and Budget |
| OMNCS | Office of the Manager, National Communications System |
| PCCIP | Presidential Commission on Critical Infrastructure Protection |
| PKI | Public Key Infrastructure |
| PSTF | Protecting Systems Task Force |
| R&D | Research and Development |
| SAFE | Security and Freedom Through Encryption |
| SSE-CMM | Security Systems Engineering Capability Maturity Model |
| U.S. | United States |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# APPENDIX D

# GLOSSARY

# GLOSSARY

| | |
|---|---|
| Audit | The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.[1] |
| Authentication | Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual's authorization to receive specific categories of information.[2] |
| Availability | Timely, reliable access to data and information services for authorized users.[3] |
| Confidentiality | Assurance that information is not disclosed to unauthorized persons, processes, or devices.[4] |
| Detection | Measures taken to identify that an intrusion has been attempted, is occurring, or has occurred.[5] |
| Deterrent | A measure taken to discourage hostile action by a threat.[6] In the context of information security, generally refers to legislation against computer crime and law enforcement efforts to prosecute computer criminals. |
| False Positive Alert | Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.[7] |
| Integrity | Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [8] |
| Intrusion | Unauthorized access to, and/or activity in, an information system. [9] This broad definition of intrusion includes unauthorized activities of both outsiders and insiders. |
| Metric | A random variable *x* representing a quantitative measure accumulated over a period.[10] |
| Mitigation | Actions taken to make the effects of an intrusion less severe.[11] Mitigation actions include provision of alternative systems, system redundancy, and system fault tolerance.[12] |
| National Security Emergency Preparedness (NS/EP) Telecommunications Services | The telecommunications services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that does or could: cause injury or harm to the population; cause damage or loss of property; or degrade or threaten the NS/EP posture of the United States.[13] |

| | |
|---|---|
| Network Security | Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.[14] |
| Non-repudiation | Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.[15] |
| Prevention | Measures taken to preclude or deter an intrusion.[16] |
| Protection Measures | For the purpose of this document, measures taken to prevent, detect, respond to, or mitigate the effects of an intrusion. |
| Redundancy | Duplication or repetition of elements in electronic or mechanical equipment to provide alternative functional channels in case of failure.[17] |
| Reliability | Assurance that systems will perform consistently and at an acceptable level of quality.[18] |
| Response | An action or series of actions constituting a reply or reaction against an attempted or successful intrusion.[19] Includes actions taken to restore a network to its full operating capability following an attack. [20] |
| Risk | Vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures.[21] |
| Security Policy | The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.[22] |
| Single Sign-On | The concept of using one login event to log a user in to several applications.[23] |
| Threat | Capabilities, intentions, and attack methods of adversaries to exploit vulnerabilities of an information system, or an information-based network, or any circumstance or event with a potential to cause harm in the form of destruction, disruption, and/or denial of access.[24] |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.[25] |

[1] *NSA Glossary of Terms in Security and Intrusion Detection,* 1998 [http://www.sans.org].
[2] *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, January 1999, (Revision 1) [http://www.nstissc.gov/assets/pdf/4009.pdf].
[3] Ibid.
[4] Ibid.
[5] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, Network Group Intrusion Detection Subgroup of the President's National Telecommunications Security Advisory Committee, Annex D: Glossary, December 1997.
[6] *Webster's II: New College Dictionary*, Houghton Mifflin Company, New York, 1995.
[7] *NSA Glossary*, op. cit.
[8] *Defense-wide Information Assurance Program Briefing (DIAP) to PSTF*, December 1, 1999.
[9] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[10] *NSA Glossary*, op. cit.
[11] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[12] *Summary of Ongoing I&C CIP R&D Programs.* Information and Communications (I&C) Subgroup of the Critical Infrastructure Protection, Research and Development, and Interagency Working Group, May 26, 1999: Attachment A.
[13] *National Communications System Manual 3-1-1, Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NS/EP) Service User Manual*, National Communications System, Washington, DC, March 1998.
[14] NSTISSI No. 4009, op cit.
[15] *DIAP Briefing*, op. cit.
[16] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[17] *Webster's II*, op. cit.
[18] *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document*, Third Edition, Office of the Manager, National Communications System, March 1999.
[19] *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, op. cit.
[20] *Summary of Ongoing I&C CIP R&D Programs*, op. cit.
[21] *NSA Glossary*, op. cit.
[22] Ibid.
[23] http://www.cybersafe/news/glossarys.html.
[24] *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications*, op. cit.
[25] NSTISSI No. 4009, op. cit.

# APPENDIX E

# REFERENCES

## REFERENCES

1. *An Assessment of the Risk to the Security of the Public Network,* prepared by the U.S. Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIE), Office of the Manager, National Communications System, April 1999.

2. Burton, CAPT J. Katharine (USN), Staff Director, Defense-wide Information Assurance Program (DIAP), Briefing to PSTF, December 1, 1999.

3. Cain, Patrick, GTE, Briefing to PSTF, January 11, 2000.

4. *Computer Hacker Information Available on the Internet,* GAO/AIMD-99-108, June 5, 1996.

5. "Critical Foundations: Protecting America's Infrastructures," President's Commission on Critical Infrastructure Protection, October 1997 [http://info-sec/pccip/web/report_sale.html].

6. *Critical Infrastructure Protection, Comprehensive Strategy Can Draw on Year 2000 Experiences,* GAO, October 1999 [http://www.gao.gov/new.items/bysubject.htm#16].

7. "Cyber Security Initiatives," The White House, Office of the Press Secretary, February 15, 2000.

8. *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk,* GAO/AIMD-99-107, August 1999.

9. *Federal Information System Controls Audit Manua*l, GAO/AIMD-12.19.6, January 1999.

10. Fraser, Barbara, Cisco Systems, Briefing to PSTF, January 14, 2000.

11. *Trends Solutions, and Ruminations*, Grance, Tim, National Institute of Standards and Technology, Computer Security Division, Briefing to PSTF, December 1, 1999.

12. Hudson, Tom, Raytheon, Briefing to PSTF, January 11, 2000.

13. *Information Security Magazine* 1999 Survey [http://www.infosecuritymag.com/july99/].

14. *Information Security Management: Learning from Leading Organizations,* GAO/AIMD-98-68, May 1998.

15. *Information Security Risk Assessment: Practices of Leading Organizations (Exposure Draft),* GAO/AIMD-99-139, August 1, 1999.

16. "Information Technology for the Twenty-First Century: A Bold Investment in America's Future: Proposed in the President's FY2000 Budget," National Science and Technology Council, June 1999 [http://www.ccic.gov/pubs/it2-ip].

17. "Information Technology Frontiers for a New Millennium," National Science and Technology Council, April 1999 [http://www.hpcc.gov/pubs/blue00].

18. "Institute from Information Infrastructure Protection," The White House, Office of the Press Secretary, January 7, 2000.

19. "Is IT Safe?" *CIO Magazine,* July 15, 1999.

20. Knode, Ron, Computer Sciences Corporation (CSC), Briefing to PSTF, January 11, 2000.

21. Lewis, Jamie, "Focus on Business Relationships to sell you IT Strategy," *Internetweek,* September 27, 1999 [http://www.technweb.com/se/directlink.cgi?INW19990927S0048].

22. Lynas, David, "Is Awareness Enough," presentation at 1999 Computer Security Institute Conference, November 16, 1999.

23. *Many NASA Mission-Critical Systems Face Serious Risks*, GAO/AIMD-99-37, May 1999.

24. Martin, Ronald A., Raytheon, Briefing to PSTF, January 14, 2000.

25. McGhie, Lynda L., Lockheed Martin, Briefing to PSTF, January 11, 2000.

26. Memorandum for the Heads of Departments and Agencies, M-00-07, From: Jacob J. Lew, Director, Chief Information Officers Council, Subject: Incorporating and Funding Security in Information Systems Investments, February 28, 2000 [http://www.cio.gov/docs/lews_lessons.htm].

27. National Communications System Manual 3-1-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NS/EP) Service User Manual,* National Communications System, Washington, DC, March 1998.

28. *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, January 1999 (Revision 1) [http://www.nstissc.gov/assets/pdf/4009.pdf].

29. *National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11,* Subject: National Policy Governing the Acquisition of Information Assurance (IA)

and IA-Enabled Information Technology (IT) Products, National Security and Telecommunications Systems Security Committee (NSTISSC), January 2000.

30. *NSA Glossary of Terms in Security and Intrusion Detection,* 1998 [http://www.sans.org/newlook/resources/glossary.htm].

31. OMB Circular A-123, 6/21/95, *Management Accountability and Control*.

32. OMB Circular A-130, 2/8/96, *Management of Federal Information Resources*.

33. Peltier, Thomas, "Security Issues for 2000 and Beyond," presentation at 1999 Computer Security Institute Conference, November 15, 1999.

34. *Pervasive, Serious Weaknesses Jeopardize State Department Operations,* GAO/AIMD-98-145, May 1998.

35. "President Seeking Increased Measures to Combat Cyber-threats," *Associated Press,* January 6, 2000.

36. Report of the Network Security Task Force, The President's National Security Telecommunications Advisory Committee, October 1990.

37. *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development,* Network Group Intrusion Detection Subgroup of the President's National Telecommunications Security Advisory Committee, December 1997.

38. Schlarman, Glen, Office of Management and Budget, Briefing to PSTF, January 11, 2000.

*39. Strengthened Management Needed to Protect Critical Federal Operations and Assets,* GAO/T-AIMD-98-312, September 1998.

40. *Summary of Ongoing I&C CIP R&D Programs,* Information and Communications (I&C) Subgroup of the Critical Infrastructure Protection, Research and Development, and Interagency Working Group, May 26, 1999: Attachment A.

41. "Survivable Network Technology," Carnegie Mellon Software Engineering Institute, September 1, 1999 [http://www.sei.cmu.edu/organization/programs/nss/surv-net-tech.html].

42. *System Security Engineering Model*, SSE-CMM, Carnegie Mellon University, April 1, 1999.

43. *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document,* Third Edition, Office of the Manager, National Communications System, March 1999.

44. *The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems Sensitive Data*, GAO/T-AIMD-99-146, April 1999.

45. *Webster's II: New College Dictionary*, Houghton Mifflin Company, New York, 1995.