PRACTICES FOR SECURING CRITICAL INFORMATION ASSETS

January 2000

Critical Infrastructure Assurance Office
1800 G Street, N.W., Suite 8-130
Washington D.C. 20006

TABLE OF CONTENTS

Acknowledgments

The U.S. Critical Infrastructure Assurance Office (CIAO) gratefully acknowledges permission to extract, condense, paraphrase, and make use of material from the following sources: Edward G. Amoroso of AT&T Labs; ICSA.net; the Board of Governors of the Federal Reserve System; Booz-Allen & Hamilton, Inc.; the Government of Canada, Communications Security Establishment; KPMG Peat Marwick LLP; and the U.S. Department of Commerce, National Institute of Standards and Technology.

The following CIAO representatives assisted in the preparation of this document: Mickey Busciglio, Fran Carnevale, Hilary Lombardo, Jerry Mulvenna, Gary Neubert, Glenn Price, Paul Rodgers, and Lee Zeichner. Anne DeMarsay acted as technical editor. Suzi Shoemake provided final formatting and editing. Sandy Scroggs designed the document's cover page.

For printed copies of this document or further information on the CIAO, please contact:

Critical Infrastructure Assurance Office
1401 Constitution Avenue, NW
Basement Mezzanine 018
Washington, DC 20230

Phone: (202) 482-7450
Fax: (202) 482-7498 / 99
Email: media@ciao.gov

This document is also available on-line at the CIAO website: www.ciao.gov

By accessing the on-line version, readers can hyperlink to the numerous sources of information on Critical Infrastructure Protection referenced in this document.

Executive Summary

In May 1998, President Clinton issued Presidential Decision Directive 63 (PDD-63), which calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructure of the United States, especially the cyber-based infrastructure. The Critical Infrastructure Assurance Office (CIAO) was established to assist in the development of a national plan for protecting the country's critical infrastructure and to coordinate plan implementation efforts. Federal departments and agencies are beginning the process of identifying and securing those critical assets and related infrastructure components that they depend on to fulfill their responsibilities of ensuring national security, national economic security, and public health and safety.

The CIAO is issuing *Practices for Securing Critical Information Assets* to provide initial guidance to Federal agencies in performing these tasks. This guidance is intended to assist agency personnel who are responsible for developing and implementing information security policy, rather than those involved in devising actual technical solutions. It is also intended to complement, not supplant, existing guidance and authority of other organizations[1] responsible for issuance of security standards and guidelines.

This guide includes chapters on establishing a security policy, identifying critical assets and performing vulnerability assessments, understanding the tools and practices available to improve security, and developing an effective incident response capability; a glossary of terms and acronyms; and appendices. As indicated in the acknowledgments, some of the information was gathered from public domain sources and condensed for inclusion. Other information was developed by CIAO personnel. Appendix A contains bibliographic references for all sources used in the preparation of the guide and additional sources of information on security that are available online.

The information in this guide is not intended to be either definitive or complete. It is a compilation of good information on the subjects mentioned above, and should be used by Federal agencies and other organizations in conjunction with information obtained from other sources to develop and implement effective policies and capabilities for protecting the nation's critical information infrastructure.

Notice: This document was prepared by an agency of the U.S. Government. Neither the United States Government nor any agency thereof, nor any of its contractors, subcontractors, or employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the content of the document or any apparatus, product, or process disclosed. Reference herein to any commercial product, process, or service by trade name, trademark,

[1] E.g., Office of Management and Budget (OMB) for information technology, the National Institute of Standards and Technology (NIST) for sensitive systems, the National Security Agency (NSA) and the National Security Telecommunications and Information Systems Security Committee (NSTISSC) for national security systems and the Chief Information Officer (CIO) council for best practices.

manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, any agency thereof, or any of its contractors or subcontractors. The views and opinions expressed herein do not state or reflect those of the entire U.S. Government or any of its contractors or subcontractors.

This paper contains hypertext links or pointers to information created and maintained by other public and private organizations. Neither the U.S. government nor the CIAO controls or guarantees the accuracy, timeliness, or completeness of any linked information. The inclusion of links or pointers to Web sites is not intended to assign importance to those sites or the information contained therein, nor is it intended to endorse or recommend any views expressed, or products or services offered on these sites.

Chapter I. Establishing Information Security Policy

Information Security Policy

Information security policy refers to the set of rules and practices an agency uses to manage, protect, and allocate its information resources. As the NIST notes in Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*:

> In discussions of computer security, the term *policy* has more than one meaning. *Policy* is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term *policy* is also used to refer to specific security rules for particular systems. Additionally, *policy* may refer to entirely different matters, such as the specific managerial decisions setting and organization's e-mail privacy policy or fax security policy.[1]

In this guide, we will be using the term *policy* in all these senses.

- *Program policy* is what management uses to create an organization's security program. It is high-level, comprehensive, and unlikely to need frequent updating.
- *System-specific policy* is the body of rules and practices used to protect a particular information system. System-specific policy is limited to the system or systems affected and may change with changes in the system, its functionality, or its vulnerabilities.
- *Issue-specific policy* addresses issues of current relevance and concern to the agency. Issue-specific policy statements are likely to be limited, particular, and rapidly changing. Their promulgation may be triggered by a computer security incident.[2]

Program Policy

In a Federal agency, the formulation of program policy must proceed within the framework of existing laws, regulations, and Executive Branch policies, including the Computer Security Act of 1987 (P.L. 100-235); OMB Circular A-130, *Management of Federal Resources* (February 8, 1996), particularly Appendix III, Security of Federal Automated Information Resources; and PDD-63, *Protecting America's Critical Infrastructures* (May 22, 1998). It must also be guided by the agency's mission statement and organizational structure. Appendix B contains an overview of the social, political, and legal history of Federal computer security and information resources management policy, followed by a list of current authorities and policy guidance.

Program policy development and promulgation is the responsibility of senior management and should take place under the direction of the agency head or senior administration official responsible for the agency. The components of an adequate program policy include the following:

---

[1] U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Developing Security Plans for Information Technology Systems*, NIST Special Publication 800-18 (Washington, D.C.: December 1998), p. 33. Much of the material in this chapter is adapted from this publication, which is available online at http://csrc.nist.gov/nistpubs/ .

[2] *Ibid*., pp. 33-34.

- *Purpose statement*. The purpose statement explains why the program is being established and what its information security goals are. Examples of goals include maintaining system and data integrity, protecting confidentiality of personal data, and maintaining availability of service. Agencies' goals will vary with their missions; the IRS, which maintains huge databases of confidential personal information, would have different security concerns than the FAA, whose computers are essential to controlling air traffic safety.
- *Scope*. The scope section should state which agency resources—hardware, software (operating systems, applications, and communications packages), data, personnel, facilities, and peripheral equipment (including telecommunications)—are to be covered by the security program.
- *Assignment of responsibilities*. The program policy document should assign responsibility for information security program management to a single office and spell out supporting responsibilities of executives, line managers, applications owners, users, and the information technology (IT) organization. Clear, specific, and complete assignment of responsibilities supports another information security goal: accountability.
- *Compliance*. The compliance section should describe how the agency will oversee the creation and conduct of the information security program and who will be responsible for enforcing compliance with system-specific and issue-specific policies. This section may also establish a disciplinary process for dealing with infractions in general terms.

System-Specific Policy

Agencies are likely to have multiple sets of system-specific policy relating to security, from the very general (e.g., access control rules about who may have user accounts) to the very particular (e.g., system permissions reflecting segregation of duties among employees involved in handling payroll). OMB Circular A-130, Appendix III requires system security plans incorporating such policies and implementation procedures, and NIST's Special Publication 800-18 provides detailed guidance on developing them.

Because of the varying scope and specificity of this type of policy, it may be difficult to determine whether the existing body of system-specific policy is adequate to meeting information security goals. NIST suggests analyzing existing policies and formulating new ones using a two-step process.[3]

- *Define security objectives for the system*, based on agency information security goals and system functional or mission requirements. These objectives should be achievable action statements. A security objective for availability might be: "Ensure 99 percent or better network availability 24 x 7 x 365 during the fiscal year." For confidentiality, an objective might be: "Reduce incidents of unauthorized access by employees, contractors, and service personnel to fewer than three per year."
- *Write operational security rules to achieve security objectives*. The degree of specificity of these rules will vary, as will their formality. Some may be implemented by setting automated system controls (for example, access control), but should be supplemented by written statements (for example, who is to be granted access privileges). Developing and

[3] *Ibid*., pp. 40-42.

implementing operational security rules will involve tradeoffs. Detailed, written policies may be clear and easy to enforce but create an administrative burden. Similarly, automated controls can make enforcement consistent but may be too rigid unless they permit an authorized manager to override them when an exception should be made.

Issue-Specific Policy

The agency's body of issue-specific policy statements is likely by its nature to lack a coherent relationship to information security goals. Individual policy statements, however, may be highly pertinent to these goals, such as those governing Internet access by users, installation of unauthorized software or equipment, and the sending/receipt of attachments to email. Agencies should begin by gathering all issue-specific policies, organizing them by topic, selecting those that appear to affect security goals for further analysis, and identifying areas where additional policies may be needed. When an issue-specific policy statement needs to be formulated or revised, NIST suggests the following structure[4]:

- *Issue statement*. This statement should include terms, definitions, and conditions; for example, what is "unauthorized software"? Include the rationale or justification for the policy if possible.
- *Statement of the agency's position*. This statement reflects management's decision on the policy; for example, "The use of unauthorized software is prohibited."
- *Applicability*. The applicability statement specifies where, how, when, to whom, and to what the policy applies.
- *Compliance*. Who is responsible for enforcing the policy? Who is authorized to grant exceptions?
- *Points of contact for information or guidance*.

Education, Training, and Awareness

Introduction

Education, training, and awareness are all necessary to the successful implementation of any information security program. These three elements are related, but they involve distinctly different levels of learning.

Awareness is not training but is a prerequisite to it. Its purpose is to focus attention on security. Awareness programs are generally well established within organizations. An example of an awareness campaign would be the plethora of posters visible in most Federal buildings, reminding users that passwords are not to be shared. Awareness provides a baseline of security knowledge for all users, regardless of job duties or position. The level of security awareness required of a summer intern program assistant is the same as that needed by the Director, Chief, or Administrator of the agency. IT security awareness programs should be tied directly to security policy development and the organization's computer security incident response capability (see Chapter IV).

[4] *Ibid*., pp. 38-39.

Training is geared to understanding the security aspects of the particular IT systems and applications that the individual uses. For example, all users need to learn the security features of the office automation software resident on their respective systems. They also need to understand the security features of the local area network (LAN) to which they are connected, as well as security issues related to connectivity to the Internet, intranet, and/or extranet. There may well be overlapping issues, but each system is a distinct entity that requires its own set of security measures. Security training should take into account the uniqueness of each system and application.

Education differs from training in both breadth and depth of knowledge and skills acquired. Security education, including formal courses and certification programs, is most appropriate for an organization's designated security specialists.

Security Awareness and Training Requirements for Federal Agencies

Security awareness and training in accepted security practices for Federal employees are mandated by the Computer Security Act of 1987 (P.L. 100-235) for "all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."[5] NIST and the U.S. Office of Personnel Management (OPM) were assigned the joint task of developing and issuing guidelines for the computer security training mandated by P.L. 100-235. NIST issued Special Publication 500-172, *Computer Security Training Guidelines*, in November 1989. In January 1992, OPM issued a revision to Federal regulations that made the voluntary guidelines in that publication mandatory.[6]

The OPM regulation requires training: (1) for current employees; (2) for new employees within 60 days of hire; (3) whenever there is a significant change in the agency's IT security environment or procedures; and (4) when an employee enters a new position that deals with sensitive information. It also requires periodic refresher training, based on the sensitivity of the information the employee handles.

OMB Circular A-130, Appendix III restates these mandatory training requirements. It also requires that *before* receiving access to any IT systems or applications, *all* employees must receive specialized training focusing on their IT security responsibilities and established system rules.

Training and Education Resources

Among the first places a Federal information system security program manager or system security officer should look for training guidance is NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (April 1998), [7] which replaces Special Publication 500-172. This document is a valuable source of information on training requirements for different job roles and responsibilities.

[5] Computer Security Act of 1987, P.L. 100-235, Sec. 5(a).
[6] 5 CFR Part 930, RIN 3205-AD43.
[7] U.S. Department of Commerce, National Institute of Standards and Technology, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST Special Publication 800-16 (Washington, D.C.: April 1998). This publication is available online at http://csrc.nist.gov/nistpubs/ .

NIST also maintains the online Computer Security Resource Clearinghouse (CSRC), where anyone can access information on training opportunities. The objectives of the CSRC include coordinating the dissemination of laws, policies, procedures, and training materials; identifying, modifying, and developing standardized training and awareness materials; and maintaining a repository of these materials. The Web address of the clearinghouse is http://csrc.nist.gov/.

Other useful Government Web sites for information on training and education include the following:

- The Federal Information Systems Security Educators' Association (FISSEA) page on the NIST site, at http://csrc.nist.gov/organizations/fissea.html.
- The Office of Information Technology's IT Policy On-Ramp on the General Services Administration's Web site, at http://www.itpolicy.gsa.gov/.
- The Defense Information Systems Agency (DISA), the Department of Defense's lead computer security organization, has an INFOSEC Education, Training, Awareness, and Products Branch that offers computer-based training (CBT) courses on information systems security. For more information, go to http://www.disa.mil/infosec/tsp.html .

In May 1999, the National Security Agency (NSA) designated seven U.S. universities as *Centers of Academic Excellence in Information Assurance Education*: the University of California at Davis, George Mason University (Virginia), the University of Idaho, Idaho State University, Iowa State University, James Madison University (Virginia), and Purdue University (Indiana). These universities offer formal courses and degree and certificate program especially suited to agency information security specialists.

Tips on Successful Policy Development and Implementation

Each agency has its own process for developing, implementing, and revising policies, appropriate to its mission and organizational structure. The suggestions below were drawn from the experience of both experts in security policy development and agency managers, and may help to make your process run more smoothly.

Policy Development and Maintenance

- Obtain senior management support, including a commitment to enforcement of security policy.
- Establish working relationships with other offices in the agency who are involved in organizational security issues, such as human resources, internal audit, facilities management, and budget and policy analysis. Don't work in isolation.
- Establish a review and approval process that includes legal and regulatory specialists, human resources specialists, union representatives, policy/procedures experts, and others appropriate to your organization and mission. Allow enough time for the review and respond to all comments received, whether you accept them or not.

- Communicate with those involved in formulation and review. Clearly mark all review documents as "draft" and make sure those involved have full notice of the review and approval process and deadlines.
- Schedule an annual review of security policy as part of yearly planning. Look at whether current rules and practices are adequate to deal with the operating environment, technology changes, and the like.
- Anticipate the need for updates, particularly in system-specific and issue-specific policies, created by changes in technology, planned IT acquisitions, and similar events.

Policy Implementation

- Get employees' and other users' attention. At a minimum, have the senior official responsible send out a notice to all employees announcing the impending issuance of the security policy. Keep employees updated on progress on the security program.
- Publish the program policy document widely, electronically and in hard copy. When the security program has been created, write a descriptive booklet for users.
- Make sure security policy and appropriate practices are taught to new and current users, whether in separate orientation and training sessions or as part of existing sessions and training programs.
- Stipulate that before a user is given access to your system, he or she must first sign and return a statement to the effect that the user has read and understood the organization's security policy, and agrees to abide by its terms. Security polls reveal that "insider" threats from disgruntled or dishonest employees constitute the number-one risk to the security of computing resources.
- Maintain awareness. Use an internal Web site, posters, newsletters, and the like to remind employees of the importance of information security. Post information security FAQs ("frequently asked questions") on the Web site. Provide an email box for comments, questions, and suggestions.

Chapter II. Identifying Critical Assets and Conducting A Vulnerability Assessment

Key Terms

Critical Asset	An asset that supports national security, national economic security, and/or crucial public health and safety activities.
Threat	Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment.
Vulnerability assessment	An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to (1) identify weaknesses that could be exploited; and (2) predict the effectiveness of additional security measures in protecting information resources from attack.
Vulnerability audit	The process of identifying and documenting specific vulnerabilities in critical information systems.

Introduction

> Water, electricity, gas, communications (voice and data), rail, aviation, and other critical functions are directed by computer controls over vast information systems networks. The threat is that in a future crisis a criminal cartel, terrorist group, or hostile nation will seek to inflict economic damage, disruption and death, and degradation of our defense response by attacking those critical networks. Director of Central Intelligence George Tenet testified to Congress: "The threat is very real."[1]

After an organization has established its security policy, the next three tasks should be to identify *critical assets*, conduct appropriate *vulnerability assessments*, and review the multitude of possible security enhancement measures, using risk management principles. These tasks are the subject of this chapter.

[1] Executive Office of the President, *Defending America's Cyberspace: National Plan for Information Systems Protection*, Version 1.0 (January 2000), pp. vii.

Task 1: Identify Critical Information Assets

Asset Inventory

The first step in determining what information systems, data, and associated assets—facilities, equipment, personnel—constitute the critical information infrastructure is to draw up an inventory of all candidate assets.

The extent to which agencies maintain up-to-date inventories of their physical assets and automated information systems—hardware, software, operating systems, peripherals—varies greatly. Some agencies may be able to start from property lists or inventories performed in accordance with the requirements of OMB Circular A-130. Others may find that they will have to conduct a separate inventory.

Identifying interdependencies among components of an infrastructure is a relatively new but crucial part of security planning. As PDD-63, *Protecting America's Critical Infrastructures* (May 22, 1998), noted:

> Critical infrastructures . . . include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private. Many . . . have historically been physically and logically separate systems that have little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have been increasingly automated and interlinked.[2]

Figure 1, *CIAO Infrastructure Asset Evaluation Survey*, may be used to identify Federal agencies' critical assets in the context of PDD-63. This survey, developed in association with Booz-Allen & Hamilton, Inc., is a valuable tool for highlighting physical and cyber assets that require in-depth analysis.[3]

There is no hard-and-fast rule for determining what is or is not a critical information asset. In general, the more goals an asset supports—and the more "significantly" answers to questions on the survey list for each goal—the more important it is. It may be helpful to rank the critical information assets you have tentatively identified in order of importance to assist you in allocating resources to their protection.

[2] Executive Office of the President, *Protecting America's Critical Infrastructures*, Presidential Decision Directive/NSC-63 (May 22, 1998), p. 1, available online at http://www.ciao.gov/CIAO_Document_Library/paper598.html .

[3] Booz-Allen & Hamilton, Inc., *Infrastructure Asset Evaluation Survey*, developed for the U.S. Critical Infrastructure Assurance Office (CIAO) under contract number 40AAEX909180 (November 1999).

"Perform Essential National Security Missions"

PDD-63 states that the United States shall maintain the continued ability "to perform essential national security missions." According to the 1998 National Security Strategy of the United States, "essential national security missions" are those activities that defend the nation's vital interests—those of broad, overriding importance to the survival, safety, and vitality of our nation, including the physical security of our territory and our allies. In this regard, the questions below seek to address the level to which the asset under review is needed to protect and safeguard the interests of the U.S. and its allies, and to affect the overall strategic and tactical posture of the United States.

Choose one box for each question below:

1. To what degree is the asset required to perform an essential national security mission?	Significantly	Moderately	Indirectly	Not at all	Unknown
2. What role does the asset play in supporting the operations and capabilities of the Department of Defense?	Lead role	Support	Indirect	Not at all	Unknown
3. What role does the asset play in supporting missions related to National Security Emergency Preparedness (NS/EP) as defined by Executive Orders 12472 and 12656?	Lead role	Support	Indirect	Not at all	Unknown
4. Is the asset directly associated with a function that is specifically mandated by the United States Constitution?	Yes		No		Unknown
5. To what level does the asset support the execution of Continuity of Government (COG) programs? ("Continuity of Government (COG) programs" refer to those specific government programs intended to ensure the survival of our Constitutional form of government in the face of a catastrophic crisis.)	Significantly	Moderately	Indirectly	Not at all	Unknown
6. To what degree would the loss or degradation of the asset limit the ability of the department/agency to continue essential operations as defined through the department's "COOP plan" in the event of a crisis?	Significantly	Moderately	Indirectly	Not at all	Unknown
7. To what degree does the President rely on the asset during crisis situations? (Please explain.)	Significantly	Moderately	Indirectly	Not at all	Unknown
8. Does the asset protect national security information, data, and/or technology as defined by Executive Order 12958 or the Atomic Energy Act? (E.O. 12958 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The Atomic Energy Act specifically defines certain information relating to uses of atomic energy as classified data).	Yes		No		Unknown
9. What role does the asset play in protecting the nation's strategic natural resources (i.e., strategic petroleum reserves, national strategic stockpile, key potable water reserves, etc) or borders?	Lead role	Support	Indirect	Not at all	Unknown
10. To what degree does the asset affect another international infrastructure that is needed to secure the Nation?	Significantly	Moderately	Indirectly	Not at all	Unknown
11. To what degree does the asset affect systems or industries that directly support the industrial war-fighting base?	Significantly	Moderately	Indirectly	Not at all	Unknown
12. Do national security related treaties, agreements, or protocols with foreign governments require the asset?	Yes		No		Unknown

Figure 1. CIAO Infrastructure Asset Evaluation Survey

"Maintain Order"

PDD-63 states that, no later than 2003, the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of "state and local governments to maintain order…" The questions below are intended to address the Federal asset's role in supporting the state and local government's ability to maintain order for its citizens. Specifically, the questions seek to determine how the absence or degradation of the Federal asset could potentially lead to civil unrest.

Choose one box for each question below:

1. What role does the asset play in providing a means to maintain order?	Lead role	Support	Indirect	Not at all	Unknown
2. On what scale does this asset affect the population?	International	National	Regional	Local	Unknown
3. Does the government require the asset to deal with widespread civil unrest?	Yes		No		Unknown
4. How does the asset protect your department's or agency's facilities, personnel, or resources?	Significantly	Moderately	Indirectly	Not at all	Unknown
5 How would the loss of this asset reduce the ability of the Nation to maintain order for the population? (If significant, please explain how.)	Significantly	Moderately	Indirectly	Not at all	Unknown
6. Are there any other equivalent assets that could be substituted for this particular asset in order to preserve or maintain order for the people?	Yes		No		Unknown

Figure 1. CIAO Infrastructure Asset Evaluation Survey (*continued*)

"Ensure Orderly Functions of the Economy"

PDD-63 states that "the United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems." As such, many Federal agency assets support the preservation and sustainment of our national economy and are required in some capacity to protect the "economic health" of the U.S. The questions below are intended to address how (if at all) the asset assists in promoting public confidence in the Nation's ability to successfully compete in global markets and provide domestic economic security.

Choose one box for each question below:

1. What role does the asset play in ensuring the orderly functions of the economy?	Lead role	Support	Indirect	Not at all	Unknown
2. What kind of national or international economic disruption would the loss or degradation of the asset cause? (Please explain.)	Economic Collapse	Significant Disruption	Minimal	None	Unknown
3. Does this asset protect sensitive economic data? (Sensitive data is generally not releasable to the public but used by the Government.)	Yes		No		Unknown
4. To what degree does this asset support the department or agency's ability to address a market failure? (If so, how?)	Significantly	Moderately	Indirectly	Not at all	Unknown
5. Does the asset support large segments of industry?	Yes		No		Unknown
6. What role does the asset play in supporting the Federal Reserve System?	Lead role	Support	Indirect	Not at all	Unknown

Figure 1. CIAO Infrastructure Asset Evaluation Survey (*continued*)

"Ensure the General Public Health and Safety"

PDD-63 states that it seeks to protect "the ability of the Federal Government to ensure the general public health and safety." This goal includes, but is not limited to, functions that ensure the physical well-being of American citizens, such as disease control, regulatory controls over dangerous and ingestible substances, storm warnings, etc. The functions addressed are those at the Federal level, not those that belong to or are delegated to the states or municipal governments.

Choose one box for each question below:

1. What kind of services for ensuring public health and safety does the asset provide?	Unique	Important but not unique	Supporting	None	Unknown
2. The asset is needed to support the physical well being for what sized portion of the population?	Large	Medium	Small	None	Unknown
3. To what level does the asset support Federal, State, local or private response to natural disasters?	Lead role	Support	Indirect	Not at all	Unknown
4. To what level does the asset support the general notification of alerts affecting general public health and safety? (Please explain.)	Lead role	Support	Indirect	Not at all	Unknown
5. Does the asset provide coordination at national and international levels for specific public health and safety services?	Yes	No	Unknown		
6. Could the loss of this asset result in death?	Yes	No	Unknown		
7. Is this asset necessary to recover from widespread health and safety crises?	Yes	No	Unknown		
8. What role does the asset play in minimizing the effects of natural disasters on the civilian population?	Lead role	Support	Indirect	Not at all	Unknown
9. Is the asset necessary to maintain the quality of healthcare for the American populace?	Yes	No	Unknown		
10. Do international treaties, agreements, or protocols related to general public health and safety require the asset?	Yes	No	Unknown		

Figure 1. CIAO Infrastructure Asset Evaluation Survey (*continued*)

"Delivery of Minimum Essential Public Services"

PDD-63 states that it seeks to protect the ability of "state and local governments to deliver minimum essential public services." "Minimum essential public services," as defined in the 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP), include water supply, emergency services, and basic government services oriented toward promoting the general public welfare. The Federal Government plays a supporting role to state and local governments in the delivery of such services; however, the Federal Government also delivers minimum essential public services. In this regard, the questions below seek to address the level to which the asset under review is needed to promote the basic level of services necessary to sustain the general public welfare.

Choose one box for each question below:

1. What role does the asset play in providing for the delivery of minimum essential public services?	Lead role	Support	Indirect	Not at all	Unknown
2. To what degree does the asset aid state and local government in their ability to deliver minimum essential public services? (If so, how?)	Significantly	Moderately	Indirectly	Not at all	Unknown
3. Is the asset mandated by public law? (If so, please cite reference.)	Yes		No		Unknown
4. Is the basic intent of the asset to provide for the delivery of minimum essential public services?	Yes		No		Unknown

"Dependency of Other Government Programs on the Department's/Agency's Asset"

Many Federal Government programs rely on the resources of other government agencies to fulfill their missions, the questions below seek to identify and characterize the level to which the asset reviewed provides support to other government agencies and/or other resources within the department or agency.

Choose one box for each question below:

1. To what degree does the asset support the missions of other government agencies? (Explain the missions and agencies in the space provided.)	Significantly	Moderately	Indirectly	Not at all	Unknown
2. To what degree does this asset rely on other government or private sector assets to carry out its mission?	Significantly	Moderately	Indirectly	Not at all	Unknown
3. To what level does the asset support any White House-led programs?	Significantly	Moderately	Indirectly	Not at all	Unknown
4. To what level does the asset support one or more "special agency" (CIA, State, FBI/Justice, DoD) programs or system(s)?	Significantly	Moderately	Indirectly	Not at all	Unknown
5. Would the degradation of this asset affect other internal department/agency assets? (If so, please explain how.)	Yes		No		Unknown

Figure 1. CIAO Infrastructure Asset Evaluation Survey (*continued*)

"Ensuring Delivery of Essential Private Sector Services"

PDD-63 states that one of the functions that it seeks to protect is "the ability of the private sector to ensure the delivery of essential telecommunications, energy, financial and transportation services" to the American people. The questions below seek to characterize the level to which the reviewed asset supports the delivery of such "basic private sector services" to the American people.

Choose one box for each question below:

1. What effect would the loss or degradation of this asset have on the delivery of essential private sector services? (Please explain.)	Cease	Moderately Disrupt	Slightly Disrupt	Not at all	Unknown
2. Does this asset ensure functioning and reliability of essential private sector services?	Yes		No		Unknown
3. To what degree does this asset support restoration of essential private sector services that have failed?	Significantly	Moderately	Indirectly	Not at all	Unknown
4. Does this asset protect sensitive and/or proprietary essential private sector service information, data, or technology?	Yes		No		Unknown
5. Does this asset ensure access to foreign-based essential private sector services?	Yes		No		Unknown

Figure 1. CIAO Infrastructure Asset Evaluation Survey (*continued*)

Task 2: Perform a Vulnerability Audit of Critical Information Assets

Performing a *vulnerability audit* involves finding and documenting the vulnerabilities in critical information assets. Pinpointing these vulnerabilities will be a time-consuming task that will require the assistance of experts in the hardware and software used (operating systems, communications, and applications). This guide contains a conceptual overview of a vulnerability audit based on a representative methodology.[4]

If the vulnerability audit or entire assessment is to be performed by a group of people outside the organization that owns the critical assets, it is important that those within the organization have realistic expectations about what the process will accomplish and understand that its quality will be directly related to the degree of cooperation that its members provide to the assessment team. We recommend holding a preassessment meeting or series of meetings to communicate to the assessors what information is critical to the organization and what systems contain that information and to reach agreement about the expected results.

Briefly, the audit process examines the adequacy of current agency *areas of control* to measure the organization's effectiveness in protecting *critical asset elements.* This comparison results in the identification of *areas of potential compromise*, which serve as categories for a comprehensive list of vulnerabilities for which additional security measures, disaster recovery plans, and/or modifications to security policy may be necessary. These terms are further defined in the sections below.

The National Security Agency (NSA) has developed programs to assist agencies in conducting PDD-63 vulnerability audits and other parts of vulnerability assessments. The NSA has developed a standard Information Systems Security (INFOSEC) Assessment Methodology (IAM) that agencies can use in several ways. First, NSA can perform an INFOSEC assessment on a resource-available basis. Second, agencies can have their information security assessors trained in IAM courses sponsored by the National Information Assurance Partnership (NIAP), a joint venture of NSA and the National Institute of Standards and Technology (NIST), and perform their own assessments. Finally, agencies can contract for an INFOSEC assessment from a list of IAM-trained contractors. Appendix C contains a summary of the program and information on requesting an assessment or training.

Areas of Control

Areas of control are the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. These include the following items:

- *Entitywide security* refers to planning and management that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and information system

[4] KPMG Peat Marwick LLP, *Vulnerability Assessment Framework 1.1,* developed under contract to the CIAO (October 1998).

security controls. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

- *Access controls* are procedures and controls that limit or detect access to critical asset resource elements (people, systems, applications, data and/or facilities) to guard against loss of integrity, confidentiality, accountability, and/or availability. Access controls provide reasonable assurance that resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. They may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.
- *Segregation of duties* entails policies, procedures, and an organizational structure established to ensure that no single individual controls all key aspects of physical and/or computer-related operations. Failure to segregate duties could allow someone to conduct unauthorized actions or gain unauthorized access to critical assets without detection. Segregation of duties is defined as the process of segregating work responsibilities to ensure critical stages of a process are not under the control of a single individual. This objective is achieved by dividing responsibilities for critical process stages between two or more individuals or groups. Dividing duties allows for the activities of one group or individual to serve as a check on the activities of the other and reduces the possibility that errors and wrongful acts will be committed and/or go undetected.
- *Continuity of service and operations* involves controls to ensure that, when unexpected events occur, critical services and operations, including computer operations: (1) continue without interruption or are promptly resumed; and (2) critical and sensitive data are protected through adequate contingency and business recovery plans and exercises. A comprehensive contingency plan will contain procedures to resolve uncontrollable changes to systems. By maintaining and testing the contingency plan, administrators can have confidence in their ability to provide continuous service to users.
- *Change control and life cycle management* procedures and controls prevent implementation of unauthorized programs or modifications to existing programs. Change control and life cycle management policies provide reasonable assurance that changes to applications will not interrupt the critical processes. Life cycle management policies guide software specifications, implementation, and testing. Change control policies govern application and system modifications for in-house and commercial packages or patches. An adequate set of policies, procedures, and techniques ensures that: (1) all program modifications are properly authorized, tested, and approved before implementation; and (2) access to and distribution of programs is carefully controlled.
- *System software controls* limit and monitor access to the programs and sensitive files that control the computer hardware and secure applications supported by the system. "System software" refers to a set of programs designed to operate and control the processing activities

of computer equipment; these programs help control and coordinate the input, processing, output, and data storage associated with all the applications that run on a system. Examples of system software include operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. A vulnerability audit of system software involves assessing:

- system software access control,
- monitoring,
- change control.

Critical Asset Elements

Critical asset elements include the following:

- *Personnel*. Staff, management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission-related services, information systems, and facilities. This may include groups and individuals external to the organization who are involved in the fulfillment of the organization's mission. Security management personnel are also included.
- *Automated information and control systems*. All electronic and telecommunications equipment, hardware, and software (operating systems, communications, and application packages), countermeasures, and/or safeguards that are part of or support critical assets.
- *Nonautomated information and control systems*. All other systems, internal and external, that are part of or support critical assets (for example, paper archives, personnel and accounting procedures, publications).
- *Data*. All data (in electronic and printed form) and other information that are part of or support critical assets. These include numbers, characters, images, or other means of storing information in forms that can be: (1) assessed by a human; or (2) input into a computer, stored and processed there, or transmitted digitally.
- *Facilities and equipment*. All facilities and equipment that form part of or support critical assets, especially those that house and support information technology (IT) assets.

Areas of Potential Compromise

The vulnerability audit reviews actions, devices, policies, procedures, techniques, and other factors that potentially place the organization's critical asset elements at risk, with an emphasis on risks to automated information and control systems. The outcome of the audit is a list of flaws or omissions in controls (vulnerabilities) that may affect the integrity, confidentiality, accountability, and/or availability of resources that are essential to critical assets.

Sources of Information

Gathering reliable information to perform a vulnerability audit requires a team to perform structured interviews and to review all the written documents available for each area of control and each critical asset element. Figure 2, *Information Needed for the Vulnerability Audit*, lists representative types of information and documentation needed to conduct the audit.[5]

[5] *Ibid.*

- Physical security plans
  - Facility
  - Vulnerability risk assessment
  - Procedures and policies
  - Modernization plans
  - Response plans and capabilities
  - Continuity of operations plans
- Personnel security plans
  - Clearance process
  - Key personnel identification
  - Organizational structure (lines of authority)
  - Continuity of operations cross-training and practice
  - Access controls rosters
  - Key element analysis
- Training plans
  - Inventory of classes
  - Physical and computer security awareness training
  - Certification and accreditation program
  - Emergency response and crisis management
- Security plans
  - Security concept of operations (CONOP) and practice for various applications and facilities
  - Security mode determination
  - Security test and evaluation
  - Emergency response capabilities and practice
- Computer plans
  - Architecture and access
  - Security and oversight
  - Training and awareness
  - Systems inventory and access control
  - Continuity of operations and reconstitution (disaster recovery)
  - System integrity monitoring and emergency response capabilities

Figure 2. Information Needed for the Vulnerability Audit

Information Gathering

Whether you plan to conduct document reviews, interviews, questionnaires, or some combination, there are certain topic areas and questions that you should ask during the audit. Figure 3, *Vulnerability Audit Questionnaire*, prepared by CIAO representatives and others, lists questions in 21 topic areas that you should consider.

Vulnerability Audit Questionnaire

1. POLICY

a. Does your organization have a written security policy?
b. Does the policy identify all individuals responsible for implementing that policy and what their duties are?
c. Does the policy identify the steps to be taken if there is a security breach?
d. Does the policy identify what information it is most important to protect?
e. Does the policy identify enforcement procedures that identify the penalties associated with a security breach?
f. Is the policy known by all individuals who have the responsibility for implementing that policy?
g. Has a security plan been developed based on the security policy?

2. RISK MANAGEMENT

a. Has an overall vulnerability assessment been performed on critical information assets? If so, how recently was it performed or updated?
b. Have vulnerabilities identified in the assessment been corrected? Are there remaining vulnerabilities that have not been addressed?

3. ACCOUNT MANAGEMENT

a. What is the procedure for establishing accounts? What level of supervisor approval is required?
b. Who has root access to the information on your systems?
c. Can accounts be accessed remotely? If so, by whom? What kind of justification is required before remote access is permitted?
d. What is the procedure for forgotten passwords?
e. What is the procedure for closing accounts when an employee terminates employment?
f. What is the procedure for monitoring inactive accounts?
g. What is the technical process by which accounts are established?

4. CONFIGURATION MANAGEMENT

a. Does your organization have a configuration control plan?
b. Does your organization have a Configuration Control Board or the equivalent to direct activities in this area? If so, does the Configuration Control Board approve and record all changes to hardware, software, and firmware?
c. Does your organization have network and system diagrams and a list of all system resources?
d. Are only authorized individuals allowed to move and install computer equipment?

(continued)

Figure 3. Vulnerability Audit Questionnaire
(Items 1 – 4 of 21)

5. AUTHENTICATION

a. What password rules are enforced (e.g., length, alphanumeric combinations)?
b. How often are users required to change their passwords?
c. Does your system use a password cracker to identify nonsecure passwords?
d. Does your organization keep a password history file?
e. Do users have unique authentication for different types of access?
f. Does your organization use authentication other than reusable passwords? If so, what is the policy for use of such authentication?

6. SESSION CONTROLS

a. Is logoff at the end of the day required?
b. Are there automatic session timeouts?
c. Can a user use a password to lock the screen?
d. Does an unsuccessful logon indicate the cause of failure?
e. Under what circumstances are accounts locked (e.g., after how many unsuccessful logon attempts)?
f. Is the user informed about the last successful/unsuccessful logon attempt?

7. NETWORK SECURITY

a. Does your organization have an Internet access policy?
b. How are network services accessed by members of your organization? Is back door access by unapproved means possible?
c. Does your organization have a firewall? If so, how is it configured? What services are accessible by external users inside and outside of the firewall?
d. Does your organization have an intrusion detection system (IDS)? If so, is the IDS knowledge base defined by the vendor, configurable by user, or both?
e. Who has external access to your organization's systems? Is your network's internal architecture hidden from untrusted external users?

8. MODEMS

a. Does your organization have a modem use policy? Is a justification for modem use required?
b. Does your organization have a list of all personnel with modem access privileges?
c. When employment is terminated, is modem access terminated immediately?
d. Are modems automatically disconnected after a specific period of inactivity?

(continued)

Figure 3. Vulnerability Audit Questionnaire
(Items 5 – 8 of 21)

9. CRYPTOGRAPHIC TECHNOLOGY CAPABILITY

a. Does your organization use cryptographic technology to protect sensitive information during transmission? Does the technology you use provide a digital signature capability for messages containing sensitive information?
b. Does your organization use cryptographic technology to protect sensitive information stored in the system and in archives?
c. Does your organization have a policy that clearly states when information is to be encrypted?

10. SYSTEM ADMINISTRATION

a. How many system administrators does your organization have?
b. Do your system administrators work full-time as system administrators?
c. Are your system administrators contractor employees?
d. Is there segregation of duties among system administrators?
e. Does each system administrator have a backup person?
f. Are program modifications approved by the Configuration Control Board required to be installed by systems administrators?
g. Is there consistency in the implementation of security procedures by system administrators in the organization?

11. INCIDENT RESPONSE CAPABILITY

a. Has your organization developed a computer security incident response capability (CSIRC)?
b. Have users and systems administrators received training on how to carry out their respective responsibilities when an incident occurs? Do they receive awareness reminders and periodic refresher training?
c. Does your organization maintain a knowledge base of past incidents and "lessons learned" for future use?

12. AUDITING

a. Is there a mandatory auditing policy in place?
b. What information is audited?
c. Is the audited information analyzed and reported on promptly and regularly?
d. Are security personnel trained in audit analysis?
e. Are the contents of audit logs protected from unauthorized access, modification, and/or deletion?
f. Is there a policy stating how long audit logs are to be retained?

(continued)

Figure 3. Vulnerability Audit Questionnaire
(Items 9 – 12 of 21)

13. VIRUSES

a. Does your organization have a policy for dealing with viruses?
b. Are virus protection procedures in place and used by members of your organization?
c. How is information about a virus distributed to members of your organization?
d. Do employees know how to recognize a virus and how to use antivirus software?
e. Do employees know who to contact when a virus occurs?
f. Is incoming software scanned for viruses?

14. CONTINGENCY PLANNING

a. Does your organization have a contingency plan for dealing with natural and manmade disasters? If so, who maintains the contingency plan and who is responsible for its implementation?
b. Does your organization have an uninterrupted power source (UPS) to increase the possibility of an orderly shutdown without loss of data?
c. Does the contingency plan identify and prioritize the resources that are most important to protect in an emergency?
d. Is the contingency plan tested periodically?

15. BACKUPS

a. Does your organization have backup policies and procedures?
b. How often are system and user backups performed?
c. Who is authorized to perform backups?
d. Are backup media stored in a secure location offsite?
e. Are backup media tested regularly for restorability/recoverability of files?
f. Can an operational capability be restored within acceptable time constraints?
g. What are the policies and procedures regarding archived data?

16. MAINTENANCE

a. Does your organization have written system maintenance policies and procedures?
b. Are only trusted personnel performing maintenance functions?
c. Is diagnostic software maintained onsite?
d. Does a security officer ensure that all sensitive data is removed from equipment before it is sent out for repair, that returned equipment has not been tampered with, and that no other security breaches have occurred when performing maintenance functions?
e. Are maintenance records kept to indicate what was done, when, and by whom?

17. LABELING

a. Does your organization have a labeling policy and procedures?
b. Is sensitive information clearly defined and labeled?
c. Are employees trained on proper labeling procedures for hard copies, electronic files, email attachments, diskettes, backup tapes and disks, and the like?

(continued)

Figure 3. Vulnerability Audit Questionnaire
(Items 13 – 17 of 21)

18. MEDIA SANITIZING/DISPOSAL

a. Does your organization have a policy and procedures for sanitizing and disposing of sensitive material on floppy disks, CDs, etc.?
b. Is it clear who is responsible for sanitizing sensitive material?
c. Is there an authority who is responsible for ensuring that media containing sensitive material are sanitized before disposal?

19. PHYSICAL SECURITY

a. Does your organization have a physical security policy and procedures?
b. Does your organization have a guard service and/or alarm system? If so, how do they work?
c. How are visitors to your organization logged in and out?
d. What are the procedures for escorting visitors? (e.g., must visitors wear badges?; are maintenance personnel escorted?)
e. Do employees sign in and out at night?
f. What are procedures for locking offices, telephone closets, and computer rooms? How are the procedures enforced?

20. PERSONNEL SECURITY

a. Is there a background check performed on new employees? If so, how is it conducted?
b. Is a background check performed on long-term employees at regular intervals?
c. Is there an orientation course on good security practices for new employees?
d. Do employees sign nondisclosure agreements? If so, under what circumstances?

21. TRAINING AND AWARENESS

a. Is there a formal information security training program within your organization? If so, is it role-based?
b. Are new Federal employees required to receive training within 60 days of hiring?
c. Are employees required to get updated security training at regular intervals?

Figure 3. Vulnerability Audit Questionnaire
(Items 18 – 21 of 21)

Task 3: Perform Risk Management Analysis

For this task, each agency should apply risk management analysis to the entire list of vulnerabilities associated with their critical assets and infrastructure dependencies. Security enhancement costs will almost always exceed available resources. Improvements, therefore, must be made according to a number of risk management analysis factors. Below are representative types of questions an agency should address before committing any of its limited resources to eliminating or reducing vulnerabilities in critical information assets.

- Can a known vulnerability be better minimized through physical or IT measures?
- How much would it cost to minimize the risk posed by the vulnerability?
- Are the security enhancement costs commensurate with the asset's overall importance?
- Do projected plans or anticipated developments suggest that the vulnerability is likely to become irrelevant in the near- to mid-term?
- How long will it take to implement fully the proposed security enhancement?
- Is it likely that advances in IT will allow the proposed security enhancement to be defeated in the near future?

The objective during this step is to minimize the known vulnerabilities associated with the most critical assets and infrastructure dependencies in an expeditious and cost-effective manner. Addressing yesterday's security concerns tomorrow will not suffice. The ideal is to address present, and if possible, future security problems today.

Chapter III. Tools and Practices for Critical Information Asset Protection

Introduction

When you prepare your agency's mitigation and disaster recovery plans under PDD-63, you will need to know not only what your vulnerabilities are, but also what you can do to prevent or reduce damage or loss from a security incident.

Computer security tools and practices are typically divided into two categories: physical security and information security. Physical security—"guns, gates, and guards"—is the starting point for any security program and the first line of defense against intrusion or damage. The measures discussed below may seem simple and obvious, but they are essential. If you must choose, make the investments needed to physically secure your site before buying high-cost information security tools. Shortchanging physical security is like equipping your car with state-of-the-art technology—then walking away and leaving your keys in the ignition and the doors unlocked.

Physical Security of Information Assets[1]

Physical security refers to the protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and accidental damage. Managers must be concerned with building construction, room assignments, emergency procedures, regulations governing equipment placement and use, energy and water supplies, product handling—and relationships with employees, outside contractors, and agencies. Some solutions may require the installation of key locks, fire extinguishers, surge protectors, window bars, automatic fire equipment, and alarm systems.

Sound Practices for Securing Facilities and Equipment

- Do not arouse unnecessary interest in your critical facilities. For example, do not include them on visitor tours.
- Make sure secure rooms have the following features:
  - Full-height walls and fireproof ceilings
  - No more than two doors. Doors should be solid, fireproof, lockable, and observable by security staff
  - Relatively small windows, all of which should have locks
  - Good key control – locking doors and windows can be an effective security strategy, as long as appropriate authorities maintain the keys and combinations.
- Keep critical systems separate from general systems.

[1] In preparing this section, the authors consulted *Safeguarding Your Technology*, NCES Publication No. 98297 (Washington, D.C.: September 1998), Chapter 5, Protecting Your System: Physical Security, published by the U.S. Department of Education, National Center for Education Statistics. This publication is available online at http://nces.ed.gov/pubs98/safetech.

- Place equipment, except for workstations, where it cannot be seen or reached from window and door openings, and away from radiators, heating vents, air conditioners, or other duct work. Place workstations in open, visible spaces to prevent surreptitious use, unless they routinely display sensitive information.
- Protect cabling, plugs, and other wires that are off the floor.
- Maintain up-to-date logs of all equipment, with serial numbers, in a secure location.
- Have plans in place for emergency repair of critical equipment.
- Mark your equipment in an obvious, permanent, and easily identifiable way.
- Identify your equipment as yours in a less obvious way as well. Label the inside of equipment with the organization's name and contact information to serve as evidence of ownership.
- Make unauthorized tampering with equipment difficult. Replace regular body case screws with Allen-type screws or comparable devices that require a special tool to open them.
- Limit and monitor access to equipment areas. Keep an up-to-date list of personnel authorized to access sensitive areas. Never allow equipment to be moved or serviced unless the task is preauthorized and service personnel can both produce an authentic work order and verify who they are. Require picture and other forms of identification if necessary and maintain logs of all service and repair activity. Train staff to err on the side of caution when dealing with outside service personnel.
- Never leave a laptop computer unattended. Secure laptops in a hotel safe rather than a hotel room, in a hotel room rather than a car, and in a car trunk rather than on the back seat. (Do not leave a laptop computer in a car trunk overnight or for long periods of time, however.)
- Keep photocopiers, fax machines, and optical scanners in public view. Because they are used for disseminating information, their use must be monitored.
- Assign shared printers to users with similar security clearances.
- Label printed information appropriately.
- Destroy sensitive waste.

Dealing with Physical Hazards

Fire

- Remove excess paper and boxes, assure that all equipment is properly grounded, and maintain an orderly environment to reduce the fire threat.
- Ensure that smoke detectors are installed near equipment. Keep fire extinguishers near equipment and train employees in their proper use. Conduct regular fire evacuation exercises.

Environmental Control Systems Malfunctions

Environmental support includes clean air, heating and air conditioning, humidity, and water, some of which may be supplied or regulated by automated control systems. Malfunctions in

environmental control systems at a computer operations center can cause equipment failures as well.

- Keep all rooms containing computers at reasonable temperatures (60 to 75 degrees Fahrenheit or 10 to 25 degrees Celsius). Keep humidity levels at 20 to 70 percent. Monitor environmental settings and install an alarm system to notify staff if temperature and humidity readings move outside a preset range.
- Prohibit eating, drinking, or smoking near computers.

Liquid Leakage

Damage may occur as a result of burst or leaking pipes or accidental discharge of sprinklers.

- Keep liquidproof covers near the equipment and install water detectors on the floor near computer systems.

Lightning

Direct lightning strikes on the facility or surges due to strikes to electrical power transmission lines, transformers, and substations can be catastrophic to computer equipment.

- Install surge suppressors, store backups in grounded storage media, and install and test regularly the uninterruptible power supply (UPS) units on your computers.

Power Outages

Disruptions in the electrical power supply that last longer than one-half hour—or the life of a UPS—can seriously affect your ability to provide normal computer service and may cause loss of data.

- Integrate the installation and testing of UPS units with controlled shutdown procedures for prolonged outages.
- Install line filters to control voltage spikes and antistatic carpeting in areas near computers to minimize damage from power fluctuations and outages.

Severe Weather and Other Natural Disasters

- Keep computer systems away from large areas of glass and off elevated surfaces. If your facility is located in a high-risk area for earthquakes, secure computers with antivibration devices.

Information Security

Information security measures are intended to protect data and software against nonphysical threats, including unauthorized access, compromise of data integrity, and denial or disruption of service (for example, an attack via the Internet). They include software and electronic tools installed at various points in the client-server architecture (firewalls, intrusion detection systems, and antivirus software), sound access control practices (password requirements, limiting access to sensitive information, and the like), and encryption.

Users want to be confident that the products that they procure meet the requirements of their security policy. One method of gaining this assurance is to use evaluated and validated software. Two organizations that provide this service are listed below.

- The National Information Assurance Partnership (NIAP), a joint venture of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), has been instrumental in creating an international standard (Common Criteria Standard) for specifying the security requirements of information technology (IT) products and evaluating them to that specification. The standard provides a framework by which commercial companies can have product claims tested by a third party and, if desired, obtain a certificate of validation from NIAP. A list of NIAP-validated products is available online at http://niap.nist.gov/cc-scheme/ValidatedProducts.html.
- ICSA.net, a commercial organization that manages security-focused consortia, publishes product certification criteria for firewall, antivirus, and cryptographic products; tests these products to determine whether they comply with these criteria; and publishes a list of conforming products. ICSA.net's criteria and list of validated products is available online at http://www.icsa.net/html/certification/.

Virus Protection[2]

A computer virus is a program that can infect other programs by modifying them to include a copy of itself, just as a biological virus invades a cell, reproduces, and breaks out of the cell to infect other cells. Virus programs, like their biological namesakes, are usually small—the simplest are only a few lines of code—and therefore easily hidden in large software packages. And like a real virus, they require a "host"—a computer program.

Viruses typically consist of three parts: a mechanism that allows them to infect other files and reproduce, a trigger that activates delivery of a "payload," and the payload itself, from which the virus often gets its name. The payload is what the virus does to the file or system (besides infecting it). Payloads range from the annoying, such as displaying a message on the screen, to the extremely destructive, such as wiping out all files on the hard drive.

Viruses are often classified by their infection mechanism. The most common type is the *file virus*, which executes when an infected file is executed (typically, a file with the extension .EXE, .COM, .BAT, or .SYS). The newer *macro viruses* infect the executable code embedded in Microsoft® Office® programs that allows users to generate macros—sequences of actions initiated by a single keystroke, such as inserting a special character or formatting a paragraph.

[2] Sources consulted in the preparation of this section include the following:

(1) Michael Alexander, *The Underground Guide to Computer Security* (Reading, Mass.: Addison-Wesley, 1996), Chapter 2, Viruses, Worms, and Other Rogue Code;

(2) Network Associates, Inc., *An Introduction to Computer Viruses (and Other Destructive Programs)*, McAfee White Paper, available online at http://www.nai.com/asp_set/anti_virus/library/white_papers.asp (*note*: there are underscores between "asp" and "set," "anti" and "virus," and "white" and "papers" in the URL); and

(3) Micki Krause and Harold F. Tipton, eds., *Handbook of Information Security Management 1999* (Boca Raton: Auerbach, 1999), pp. 503-514.

Viruses may deliver their payloads as soon as they enter a system via an infected file or lie dormant until activated. During the dormant period, however, these viruses *are* reproducing and infecting clean files. Common triggers include dates (for example, the trigger for the Michaelangelo virus was March 6), the number of times a file is accessed, or a specific, common sequence of keystrokes, such as "123," the MS-DOS® sequence used to start Lotus 1-2-3®.

There are three common variants on computer viruses that share their destructive power, but lack their ability to reproduce and attach themselves to new files. *Worms* are like viruses in that they are also small, malicious programs designed to alter or destroy data. Although they cannot replicate, one copy of a destructive worm, such as the recent Worm.ExploreZip, is enough to destroy all the data on a hard drive. *Trojan horses* are destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by email or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board. *Logic bombs* contain coding similar to that used to activate dormant viruses and are usually set to cause maximum destruction. A disgruntled employee may set a logic bomb to activate and destroy data after he or she has left the organization. Criminals or malicious hackers (often called "crackers") may use them to hold software hostage and demand a ransom: "Pay up or we'll destroy your data."

At the dawn of the PC age, when standalone computers were the rule and few people used the Internet, computer viruses and their relatives were uncommon. Infected files had to be passed from one computer to another on diskettes or other media. Networking increased our vulnerability to viruses; a user inserting a diskette with an infected file into a desktop PC can now introduce a virus that will spread to all similar files on the network server.

Since the advent of Internet email and widespread use of the World Wide Web, malicious programs have become a major security threat. Viruses and worms can be transmitted around the world in a short time by attaching infected executable files to email messages. The attachments are usually Trojan horses masquerading as something the recipient has requested or would like to see, and may appear to be coming from a known source. The recent Melissa virus, for example, was transmitted via an infected Microsoft Word® file purporting to be information requested by the recipient. The file actually contained a list of pornographic Web sites—and the virus. When the file was opened, the virus reproduced and sent copies of the Trojan horse message and file to the first 50 people in the victim's email address book.

The best defense against these programs is a combination of management practices and the use of antivirus software on all servers, workstations, and laptops. Complete antivirus software includes a virus scanner that tests files and directories for the presence of viruses, including email attachments; a "disinfectant" to remove viruses from infected files; real-time protection against viruses that may hide in a computer's memory; and a subscription service for updates to the engine and virus signature files to maintain protection as new viruses are created and discovered. Major vendors now offer updates via secure channels using "push" technology and software that automatically installs the update files at a scheduled time or upon user request. Update files can thus be delivered to your servers and desktops automatically as they become available and promptly installed.

Because updates are issued as often as once a week, the automatic delivery and installation option maintains maximum protection while saving technical support staff and system administrators a good deal of time. There is a security tradeoff, however. A hostile party could take advantage of your reliance on the antivirus software vendor's good name to "spoof" you into accepting a Trojan horse masquerading as an update. Technical support staff should always review update files and patches before installing them. For maximum safety, forego the convenience of "push" technology and have your security staff download update files and patches directly from the manufacturer's Web site via a secure connection.

Sound Practices for Virus Protection

- Train users to scan all removable storage media, including new diskettes, and downloaded files before using them for the first time. Prohibit users from installing their own software on systems supporting critical information assets. Even shrink-wrapped commercial software may contain viruses.
- Have your technical support staff monitor your antivirus software vendor's site and public sites for information on new viruses and destructive programs. Issue an alert to all users if a particularly virulent or fast-spreading virus is discovered and take the preventive measures recommended by your vendor at critical entry points, such as the email server and firewall or proxy server. Public sites funded by the Government that issue advisories alerting users of the Internet to new viruses include the following:
  - http://www.fedcirc.gov. The Federal Computer Incident Response Capability (FedCIRC) "provides a central focal point for incident reporting, handling, prevention and recognition. The purpose is to ensure the Government has critical services available in order to withstand or quickly recover from attacks against its information resources." This site includes virus advisories and other resources.
  - http://www.cert.org/other_sources/viruses.html. This site is maintained by the Carnegie Mellon University's Computer Emergency Response Team. (*Note*: there is an underscore between "other" and "sources" in the URL above.)
  - http://afcert.csap.af.mil/virus.html . This Air Force site has a list of links to other virus monitoring sites.
- Develop and use consistent routines for backing up data on critical systems, using a reliable backup technology and clean, functioning media. Test backup media frequently to ensure that data is being recorded properly and files can be restored if necessary. Store archive copies in a physically secure location offsite.
- Keep your virus protection software up to date, using the updates and patches supplied by the vendor.

Patches

As software vendors find errors or flaws in their products that create a security vulnerability, they issue corrections in the form of a *patch* or *work-around*. A *patch* is a program modification that fixes an error in software that is installed on your system. A *work-around* is a temporary method of fixing or getting around the problem. A work-around is usually suggested when a patch is not available, as is often the case when vulnerabilities are first discovered.

Most vendors maintain Web sites from which current patches can be downloaded for installation. Some sites can discern what version of what product is running on a particular system, list the needed patches, and automatically download and install them.

Vulnerability Scanners[3]

Vulnerability scanners perform rigorous examinations of systems to identify weaknesses that might allow security violations. These products use two techniques for performing these examinations. First, *passive*, host-based mechanisms inspect system configuration files for unwise settings, system password files for weak passwords, and other system objects for security policy violations. These checks are followed, in most cases, by *active*, network-based assessments that reenact common intrusion detection scripts and record system responses to the scripts.

The results of a vulnerability scan correspond to a snapshot of system security at a single point in time. Although these tools cannot detect an attack in progress, they can determine whether an attack is possible, and in some cases, whether an attack has already occurred.

Firewalls[4]

A *firewall* is an access control mechanism that acts as a barrier between two or more segments of your network or overall Information Technology (IT) architecture. You may put a firewall between any or all of the following:

- The Internet and your agency's Internet servers
- Your agency Internet sites and internal networks
- Intranet network segments

Physically, a firewall consists of one or more routers and host machines with filtering software—software containing a series of rules that accept or reject packets of information, connection types or application specific communications attempting to cross the firewall. Various firewall architectures, described below in more detail, are used to perform the following functions:

- *Address screening*. Address screening ensures the delivery of only properly addressed messages and filters out messages from known, undesirable sources.
- *Network isolation*. A firewall can isolate an Internet site, internal network, or critical segment of an intranet from less secure networks or network segments. It can also conceal internal network design from outsiders.

---

3 Rebecca Bace, An Introduction to Intrusion Detection and Assessment, prepared for ICSA.net, p. 12; available online http://www.icsa.net/html/communities/ids/White%20paper/index.shtml (Note: document requires Adobe® Acrobat® Reader).

4 Material in this section is drawn from two sources available online:

(1) Board of Governors of the Federal Reserve System, "Sound Practices Guidance for Information Security for Networks," Federal Reserve Board Supervision and Regulation Letter SR 97-32 (SUP) (September 1997), in .pdf format at http://www.bog.frb.fed.us/boarddocs/SRLETTERS/1997; and

(2) Canadian Communications Security Establishment (CSE, the Canadian Government's lead IT agency), "Government of Canada Firewall Frequently Asked Questions," at http://www.cse-cst.gc.ca/cse/english/faq/firewall.html .

- *Application screening*. This level of screening limits the types of messages allowed into internal networks or network segments and excludes file types that could be exploited by intruders trying to gain control of an internal network, or steal or destroy information.

Firewall Architecture and Functionality

There are several common types of firewalls, each of which performs slightly different functions. In practice, these devices are usually used in some combination, in a firewall complex, according to the security needs of the organization and the architecture of its systems. Firewalls are generally configured to be transparent to internal users; that is, these users do not have to stop at the firewall, identify themselves, and have their identities verified before they are allowed access to resources outside the firewall. Such firewalls are more useful in keeping intruders out than in preventing attacks from within.

The simplest and least expensive type, which stops messages with inappropriate network addresses, is called a *packet filtering firewall*. It consists of a screening router and a set of rules that accept or reject a message based on information in the message's header (a packet): the source address, the destination address, and the port. A packet filtering firewall may, for example, have rules to screen out messages that originate from external sources but purport to be from internal sources ("spoofing" attempts).

A *bastion host* is the type of firewall used to separate secure sites, networks, or network segments from less secure areas. All external messages are sent to a server that acts as a bastion host, using a publicly available address. The bastion host then converts the public address to internal names or addresses on the protected network. Intruders are thus prevented from gaining access to internal names or addresses.

The bastion host also generates audit trails of all network-related activity for monitoring and intrusion detection purposes. Audit reduction software can be used to scan audit trails or activity logs to look for abnormal usage patterns, such as multiple attempts to enter a user's password, and send an alert to a system administrator's console (see the section on Intrusion Detection below).

A third type of firewall device is the *proxy server*. A proxy server runs a "proxy" version of an Internet application, such as email, and filters messages according to a set of rules for that application. For example, a proxy email server can unpack email attachments and scan them for viruses, using standard antivirus software, before they are sent to an internal user. Separate proxy servers are typically used for each application.

What Firewalls Can and Cannot Do

A firewall can provide the following types of protection to internal networks:

- Blocking unauthorized incoming traffic
- Directing incoming traffic to the public servers or internal network(s) as appropriate
- Hiding vulnerable systems from the Internet
- Logging traffic to and from the internal network(s), providing an audit and alarm system for intrusion detection

- Hiding information like system names, network topology, network device types, and internal user IDs from the Internet
- Providing more robust user authentication than standard applications

Firewalls *cannot* protect internal systems from the following security breaches:

- Viruses and similar types of malicious code, whether transmitted via the Internet or by sharing infected files
- Accidental or deliberate disclosure of information by authorized users
- Illicit use or modification of data by authorized users
- Unauthorized access to systems or information by anyone who is already "inside" the firewall; that is, a user who has been granted access to the internal network or networks
- Threats to the integrity of information that arise before data reaches the firewall or after it leaves the internal network(s)

Selecting a Firewall

The security requirements you develop based on the results of the vulnerability assessment and your agency's information and computer security policy should guide you in choosing a cost-effective firewall product that will meet your needs.

Sound Practices for Using Firewalls

- Use a firewall as part of an overall security solution when the value of the information or service to be protected justify the cost. Remember that it is not a "silver bullet."
- Make the firewall the *only* connection between the internal network(s) and outside resources such as the Internet. Eliminate any back door methods of access such as unauthorized modems.
- Perform necessary maintenance tasks after the firewall has been installed. The three main tasks are to:
  - *Review audit trails and activity logs generated by the bastion host to improve intrusion detection*. These logs are of no value unless used. Establish the required frequency for review in your system-specific security policy and enforce it. Note unusual patterns of usage and investigate them. Follow up on alerts generated by the firewall.
  - *Reconfigure the firewall as applications, protocols, and users change and as systems are upgraded or reconfigured*. Invest the time necessary to maintain a working firewall that accurately reflects security policy.
  - *Test the firewall regularly to ensure that it is performing as expected.*

Intrusion Detection Systems[5]

Intrusion detection systems (IDSs) are software packages that collect information from a variety of system and network sources, analyze the information stream for signs of misuse (attacks originating within the system or network) or intrusion (attacks or attempted attacks from outside), and report the outcome of the detection process. IDS reports, which may be accompanied by an alarm, generally need to be evaluated by technical support personnel before any preventive action is taken. In some cases, however, an IDS may be programmed to respond automatically to detected activity, providing *on-the-fly prevention*. Typical IDS functions include the following:

- *Monitoring and analysis of user and system activity*. An IDS typically allows the customer to build a profile of normal and/or abnormal behavior that constitutes a knowledge base against which to measure suspicious activity.
- *Assessing the integrity of critical system and data files*. File integrity assessment tools included in an IDS use strong cryptographic checksums to make tampering evident and, in the event of an attack, quickly ascertain the extent of damage.
- *Recognizing activity patterns involved in known attacks*. These activity patterns are often called *attack signatures*. An IDS typically contains a database of attack signatures, much as a virus protection software package contains a database of known virus code.
- *Performing statistical analyses to spot abnormal activity patterns that may indicate an attack or impending attack*. For example, an IDS could detect and report high system usage during a period of normally low usage.
- *Managing the operating system audit trail and alerting system managers to user behavior that violates security policy*. Examples include repeated unsuccessful logon attempts or attempts by an unauthorized user to perform system administrator functions.

Intrusion Detection Systems vs. Firewalls

An IDS is a logical complement to a network firewall that provides additional protection, particularly against threats originating from inside the firewall. Unlike a firewall, an IDS alert generally requires human evaluation of the threat and manual intervention to stop an attack. On the other hand, the more subtle and complex rules that an IDS uses to analyze system activity allow it to detect vulnerabilities and intrusions that a firewall may miss, including:

- *Attacks and security violations by authorized users of the internal network or network segments*.
- *Attacks that bypass the firewall.* Examples are *tunneling* and *application-based attacks*. *Tunneling* is the practice of encapsulating a message that would be rejected by the firewall inside a second message that will pass through it. It resembles the Trojan horse technique used to disseminate viruses. *Application-based attacks* exploit vulnerabilities in applications by sending packets that communicate directly with an application. For example, an intruder

[5] Material in this section is drawn from two sources:

(1) Edward G. Amoroso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response* (Sparta, N.J.: Intrusion.Net Books, 1999); and

(2) Rebecca Bace, *An Introduction to Intrusion Detection and Assessment*, prepared for ICSA.net (see Footnote 3 for online availability).

could exploit a problem with Web software by sending an http:// command. If the firewall is configured to pass http:// message traffic, the packet will pass through.

Intrusion Detection System Architecture

The exact architecture of an IDS will vary according to its vendor and target system. Edward Amoroso of AT&T Laboratories, a leading intrusion detection expert, lists seven primary components of an intrusion detection system, as follows:

- *Sensors*, also called probes, monitors, feeds, or taps, provide information about the system or network targeted for intrusion detection.
- *System management* refers to network management functionality embedded in the IDS. This functionality may be centralized or distributed, and is often based on network management tools such as Simple Network Management Protocol (SNMP) and the Remote Monitoring Management Information Base (RMON-MIB).
- The *processing engine* is the heart of the IDS. It consists of the instructions (language) for sorting information for relevance, identifying key intrusion evidence, mining databases for attack signatures, and decision-making about thresholds for alerts and initiation of response activities.
- *Knowledge bases* provide the means for creating user and system normal/abnormal activity profiles, capturing and storing new attack signatures, and storing any other information useful for intrusion detection.
- *Audit/archive* tools organize and provide for the storage and protection of information gathered by the sensors.
- *Alarms* typically alert a system administrator to suspicious activity or a security violation by a message, email, or page.
- The *graphical user interface (GUI)/display* is the display of intrusion detection information that appears on the system administrator's console .

What Intrusion Detection Systems Can and Cannot Do

According to ICSA.net, a current IDS can offer the following benefits:

- Increase the integrity of the rest of your security infrastructure by monitoring firewalls, encrypting routers, key management servers, and critical files.
- Interpret the mass of information contained in operating system audit trail logs and other system logs.
- Trace user activity from the point of entry to the point of exit or impact.
- Recognize and report alterations to data files.
- Recognize when a known type of attack is perpetrated on your system.
- Relieve system administrators of the task of monitoring reports of new attack signatures by providing vendor updates to databases of known attacks.
- Make expert security management of your systems by nonexpert staff possible.
- Act as a compliance engine for your security policy.

An IDS *cannot* do the following:

- Act as a "silver bullet," compensating for weak authentication and identification mechanisms (see the Access Control section below), weaknesses in network protocols, or lack of a security policy.
- Conduct investigations of attacks without human intervention.
- Analyze all the traffic on a busy network or compensate for receiving faulty information from system sources.
- *Always* deal with problems involving packet-level attacks (e.g., an intruder using doctored packets that elude detection to launch and attack, or multiple packets to jam the IDS itself).
- Deal with high-speed Asynchronous Transfer Mode (ATM) networks that use packet fragmentation to optimize bandwidth.[6]

Sound Practices for Using Intrusion Detection Systems

- Integrate the IDS with other security management features on your system or network. Use it as a complement to a firewall, not a substitute for it.
- Use the IDS as a means to help enforce your organization's security policy as well as an indication and warning system for outside attacks. You can then identify the users accessing sensitive records after hours as well as the hackers attempting an attack on your firewall.
- Establish procedures for responding to and investigating alerts or alarms received from the IDS (see Chapter IV on establishing an incident response capability). Never ignore an alert—it is better to err on the side of caution and assume you are under attack.
- Capture and store information acquired about actual attacks and security breaches in a knowledge base for use in recognizing future incidents. This knowledge base is usually created by the IDS vendor but should allow additions by the user organization. The more extensive the knowledge base, the more precisely the IDS can evaluate a possible attack.

Access Control

The purpose of access control systems and practices is to protect information from the threats of unauthorized disclosure, modification, or destruction. Access controls fortify the "CIA" of information—confidentiality, integrity, and availability—by identifying and authenticating both data and users.

Access control is a broad topic that incorporates many basic security practices. Physical access controls were discussed in the Physical Security section above. Information security-related access controls fall into two categories: (1) *technical controls*, such as passwords and encryption, that are part of normal network security; and (2) *administrative controls*, such as segregation of duties and security screening of users. These types of access control may overlap with other personnel and information security policies and procedures. In this guide, we have chosen to present a limited number of sound practices involving technical and administrative controls that we believe will be most useful in managing critical information systems.

[6] Bace, pp 16-20.

Sound Practices for Information Security-Related Access Control[7]

- *Use strong authentication to restrict access to critical systems and processes and sensitive data; control remote access to networks; and limit access to the control functions of critical network devices.* Strong authentication methods include, but are not limited to, one-time passwords, digital certificates, and biometrics.
  - *One-time passwords* are used only once and change for each user access session. These passwords are generated by programmable devices, usually chip cards (also known as smart cards or tokens). Access to the programmable device may be controlled by a reusable password for additional protection.
  - *Digital certificates*, which are discussed further in Appendix D, authenticate the identity of the user.
  - *Biometrics* refers to an identification process based on physical or behavioral characteristics unique to a user, such as fingerprints; keystroke patterns; patterns associated with the voice, retina, or iris; and facial characteristics. Commercial biometric products are available but not yet widely used. Biometric technology may offer valuable additional security measures that warrant implementation in the future to protect critical information systems.
- *Segment networks to prevent interception of data*. Because internal networks are susceptible to sniffers and other techniques for intercepting sensitive data, separate internal networks into segments so that dissemination of data is restricted to a controlled subset of users. Physically separate networks with bridges, routers, firewalls, or other access control devices to prevent users from intercepting data on segments which they are not authorized to access.
- *Change all default passwords on critical network components.* Vendors typically deliver firewalls, servers, and other critical network components with default passwords that are either listed in the product documentation or can be guessed easily by attackers. Change *all* of these passwords immediately.
- *Centralize all critical devices supporting internal local and wide area networks in secure areas to enhance physical access control*. Denying attackers physical access to critical systems and their consoles (i.e., the keyboards or workstations used to control the servers) significantly decreases opportunities to penetrate the system and/or gain a level of access that circumvents the system's security controls. Maintaining good physical access control is most easily accomplished by centralizing all critical network devices, firewalls, and servers in areas that are physically and environmentally secure and may be staffed 24 hours a day. Centralizing servers also allows more effective maintenance of server functionality, since distributed servers are often unattended after business hours.
- *Limit control of servers to local consoles in the secure area*. To discourage console-based attacks on servers, particularly attempts to retrieve restricted data such as password files, limit access of server-control devices to consoles physically attached to servers located in secure areas. This allows strict control of physical access to the console.

[7] This section is based on "Sound Practices Guidance for Information Security for Networks," Federal Reserve Board Supervision and Regulation Letter SR 97-32 (SUP) (September 1997), pp. 16-23. See Footnote 4 for online availability.

- Password-protect the console screens, and change each password often.
- If it is necessary to remotely administer servers, use strong authentication and encrypted sessions to control access by the remote device.

- *Centralize the connection points of an organization's network in secure locations*. Physically secure and closely monitor network connection points, as they are vulnerable to sniffing. Install network connection points in physically secure closets or rooms with other critical network devices.
- *Create and maintain security profiles for all users*. Security profiles define users' access to facilities and data based on their job responsibilities. They streamline the process of granting and revoking access rights to facilities and data by grouping rights together according to job function. When employees change jobs, changing their security profiles promptly is essential to preventing continued access to facilities and data that are no longer appropriate. When employees leave, promptly delete all of their access rights.
- *Protect against loss or corruption of critical process logic and sensitive data residing on desktop systems*. Because of the susceptibility of desktop systems to theft, access by unauthorized personnel, and destruction or failure, transfer storage of sensitive data or critical processes on desktop systems to servers located in secure areas. If business reasons require sensitive data or critical processes to reside on desktop systems, protect them by access controls, encryption, and periodic backup procedures.
- *Control access to desktop systems connected to critical networks or network segments, and to desktop systems supporting sensitive data or critical business processes, by a power-on logon ID/password combination or locked office*. Most desktop systems have a feature that requires a password to gain access when the device is powered up. Implement this feature to prevent unauthorized personnel from gaining control of desktop systems connected to critical networks or network segments, and those supporting sensitive data or critical processes.
- *Provide a central dial-in and dial-out modem pool for remote access*. Strictly control outside access from networked desktop systems that connect to the public-switched network. Network-connected desktop systems with modems that make calls to and from the public-switched network represent one of the greatest vulnerabilities to internal networks. Many organizations' security safeguards can be circumvented by an attacker who gains access to and control of a network-connected desktop system via an external modem. Virtually all laptop computers have modems in them, and there is a growing trend toward using laptops as desktop systems as well through docking stations.
  - Provide remote access to networks by modem pools that are isolated from the internal network via firewalls and/or other appropriate security measures. Prohibit the use of individual modems attached to networked desktop systems.
  - Shorten the standard 16-minute period that modem-pool controllers use to time out dial-in connections that are unexpectedly disconnected. During the time-out period, an attacker who gained access to the modem to which the disconnected line was attached would have the same access privileges as the authorized user who lost the connection.
  - Periodically *war-dial* all the numbers on an organization's telephone exchange to detect and eliminate unauthorized modems. *War-dialing* means dialing each number on a telephone exchange either sequentially or randomly to detect the existence of modems.

- *Consider implementing time-of-day controls for access to desktop systems connected to critical networks or network segments to eliminate unauthorized after-hours network access.* To prevent after-hours access to critical networks by unauthorized personnel, allow access to desktop systems connected to these networks or network segments during business hours only. (You will need to adjust the hours during which access is permitted by time zone and implement other access control mechanisms for remote users.) If authorized users need to use desktop systems connected to critical networks or network segments after normal business hours, grant access on an exception basis.
- *Equip desktop systems with an automatic time-out feature that makes them inaccessible to an unauthorized individual after a period of keyboard inactivity*. Simple examples of time-out features are password-protected screen savers and automatic logoffs. The length of the period of inactivity triggering the time-out feature should be determined by the sensitivity of the application.
- *Require periodic reauthentication of users during sessions involving sensitive information to ensure that the sessions have not been hijacked*. *Hijacking* occurs when an attacker disables a user's desktop system after an authenticated session with a database or system has been established, intercepts responses from the application, and responds in ways that prolong the session. The user whose desktop system has been disabled may not take action to determine the cause of the lost session soon enough to prevent the hijacker from accessing the data or system. The hijacker's access can be limited by requiring periodic reauthentication for the continuation of the session.
- *Control utility programs that provide unrestricted access to sensitive data*. Some utility programs provide unrestricted access to system commands and data to "superusers" (e.g., system administrators). When implementing software that gives superusers these capabilities, provide compensating controls, such as segregation of duties to limit their capability for autonomous actions. As an additional precaution, review logs of all superuser actions frequently.
- *Provide the same level of physical and logical access control to backup files of sensitive data, particularly those stored at offsite locations, as you provide to the versions on the system*.
- *Permanently remove all sensitive files from hard drives before disposing of obsolete desktop systems*. Erasing files is not adequate. Use commercially available software to ensure that all traces of files have been eradicated beyond recovery. Depending on the sensitivity of the data, consider physically destroying old hard drives before disposal.
- *Password-protect access to notebook and laptop computers and consider encryption of all sensitive files on these computers' hard drives*. Because portable computers are easy to steal, minimize opportunities for thieves to obtain sensitive information that may be stored on them. The first line of defense is to require a logon ID/password combination to gain access to the PC's operating system. Encrypt sensitive files so that even if the portable computer is stolen and successfully penetrated, the thieves cannot access the data. See the section above on Physical Security for tips on theft prevention.

Password Policies

Password policies are a subset of access controls. Although access to sensitive information on critical information systems is best controlled by strong authentication, reusable passwords may be adequate for controlling access to less sensitive information, as long as robust password policies are in place. In many instances, access may be controlled by a combination of strong authentication and reusable passwords.

- *Establish an effective password policy*. A password policy should include the following items:
  - A minimum length for passwords and instructions on acceptable combinations of numbers, letters, and symbols. Use for example, a password with a minimum of eight characters and at least one character from each of these categories: alpha, numeric, and special characters. Users should also be cautioned to avoid obvious or easily guessed combinations, such as names of family members or pets, birth dates, or common words in other languages.
  - Use of an automatic system prompt that requires users to change their passwords after a specified period of time or number of uses. The system should require more frequent changes in passwords for users with extensive access privileges (e.g., system administrators).
  - A prohibition on users' sharing their passwords with anyone and on writing down passwords.
- *Encrypt reusable passwords in transmission and storage*. Because of the susceptibility of networks to sniffing, hijacking, Trojan horses (see the section on Virus Protection above), and other attacks, encrypt reusable passwords in storage and in transit through the network or use one-time passwords. (See the section below on Cryptography.)
- *Select security subsystems and applications that provide a password history to prevent the reuse of recent passwords*. The password history can bar reuse of recent passwords based on either a period of time (e.g., no reuse of passwords used within the last year) or a specified number of previously used passwords (e.g., no reuse of the last 10 passwords).
- *Use commercially available applications to test the validity of users' passwords*. Applications (often called "password crackers") are available that will test for users' passwords that are easily guessed. Use these applications to screen users' passwords as they are created to ensure, for example, that no passwords are used that match words in the dictionary and therefore are susceptible to "dictionary attacks."
- *Disable user accounts after a preset period of inactivity; purge them after a longer period of inactivity*. To ensure that a system does not contain old, unused user accounts, deactivate any account that has not been used within a period of time set forth in your security policy. If you do not receive a request for reactivation, purge the account from the system. Before purging an account, however, check with the owners of the resources to which the user whose account is to be purged had access, to ensure that irreplaceable files or information are not destroyed.

- *Provide mechanisms to reduce the number of unsuccessful logon attempts. Two examples are:*
  - *Delay logon prompt after unsuccessful attempt.* Apply a delay before logon prompt that increases with each unsuccessful attempt. This will serve to eliminate numerous repeated attempts, while not disabling the account and requiring administrative action for authorized use.
  - *Disable user IDs after multiple unsuccessful logon attempts, and notify the security administrator when this threshold is reached.* To prohibit attackers from using automated programs that attempt to guess a user's logon ID/password combination, implement a threshold after which the logon ID is disabled. Be careful that the application of this practice does not open the organization up to an effective denial of service attack.
    - Have the system alert the system administrator when the threshold is reached to allow investigation of the situation.
    - Review logs to detect multiple attempts at guessing users' passwords that avoid reaching the threshold in any one session.
- *To help users detect whether someone has illicitly obtained a valid password, display the date and time of the last successful logon each time the user signs on.* Train users to observe this date and time and to report any anomalies.

Cryptography

Cryptography is the science of transforming data so that it is interpretable only by authorized persons. Data that is unencrypted is called *plaintext*. The process of disguising plaintext data is called *encryption*, and encrypted data is called *ciphertext*. The process of transforming ciphertext back to plaintext is called *decryption*.

When interception, theft, or destruction of information is a likely threat, encryption can provide an additional layer of protection to systems. While a full discussion of cryptography and encryption software is beyond the scope of this guide, this section provides an introduction to cryptographic technology and its uses.

Cryptography relies upon two basic components: an *algorithm* and a *key*. Algorithms are complex mathematical formulae, and keys are strings of bits used in conjunction with algorithms to make the required transformations. For two parties to communicate, they must use the same algorithm or algorithms that are designed to work together. In most cases, algorithms are documented, and formulae are available to all users (although the algorithm details are sometimes kept secret). Some algorithms can be used with keys of various lengths. The greater the length of the key used to encrypt the data, the more difficult it is for an unauthorized person to use a trial-and-error approach to determine the key and successfully decrypt the data.

There are two basic types of cryptography: symmetric and asymmetric. Each has advantages and disadvantages. Most current cryptographic applications combine both techniques to exploit the strengths of each type.

In *symmetric-key cryptography*, two or more parties share the same key, which is used both to encrypt and decrypt data. A third party who gains access to the key can decrypt all data that has been encrypted with that key. If you use only symmetric-key cryptography to provide a cryptographic service, the key must be securely transferred to everyone authorized to use it and this process must be repeated whenever the symmetric key changes. The most widely used symmetric-key algorithm is the Data Encryption Standard (DES), developed by IBM in the late 1970s. NIST is currently in the process of selecting a replacement algorithm to form the basis of an Advanced Encryption Standard (AES).

Asymmetric-key cryptography (also called *public-key cryptography*) is based on a mathematical discovery in the 1970s: there exist pairs of numbers such that data encrypted with one member of the pair can be decrypted by the other member of the pair and by no other means. The number made known to the public is called the *public key*; the number kept secret is called the *private key*. If the numbers are large enough, it is extremely difficult, if you know one member of the pair, to determine the other member. This allows the owner of a key pair to widely distribute the public key as long as he or she is careful to keep the private key secret. Anyone who has access to the public key can encrypt data, but only the holder of the private key can decrypt it. Anyone with the public key and decrypt data encrypted with the private key has assurance that the sender was the holder of the private key. The most widely deployed asymmetric encryption algorithm is the RSA algorithm, named for the three people who invented it: *R*ivest, *S*hamir, and *A*delman.

A disadvantage of asymmetric-key cryptography is that it is much slower than symmetric-key cryptography and is therefore impractical for use in encrypting large amounts of data. It can, however, be combined with symmetric-key cryptography to provide a secure and efficient cryptographic service. The hybrid solution is to encrypt plaintext data using a symmetric key, place the symmetric key in the header block of the transmitted data, and encrypt the header block using the public key of the data recipient. If the data is being sent concurrently to more than one person, each recipient will have a different header block, because each has a unique public key. Using this solution, a new symmetric key can be assigned for each data transmission.

Asymmetric-key cryptography also can be used to provide an authentication service, including a *digital signature service* that guarantees the identity of the originator of the message, an *accountability* (*nonrepudiation) service* that prevents the originator from denying authorship at a later date, and an *integrity service* that guarantees that the message has not been modified since it was signed by the message originator. All of these services work as follows: when the message originator requests that a message be signed with a digital signature, a computer application creates a *message digest*. The application uses a standard algorithm to compress the contents of the message into several bytes, in such a way that if the message were later to be modified, the message digest would also change. The compression algorithm also makes it impossible to recreate the message from the message digest. The message digest is placed in a *message header*, which is then encrypted with the private key of the message originator.

When the message reaches the recipients, their corresponding computer application decrypts the message header to obtain the message digest, using the public key of the message originator. The

application also uses the standard compression algorithm on the message contents to generate a second message digest. If the message digest that is generated by the recipient's computer matches the message digest that was generated by the originator's computer, the recipients are assured that: (1) the purported message originator actually sent the message; and (2) the message was not modified during transmission.

Another use for asymmetric-key technology is to encrypt and digitally sign data that is passed between a client and a server. In this case, the public key information that is exchanged belongs to the client computer and the server, not to individual users.

For asymmetric-key cryptography to work, there must be a mechanism by which users can distribute their public keys and obtain others' public keys. Users must also receive assurance that the public key they are given does indeed belong to the ostensible owner. Finally, users need a mechanism to recover data encrypted with their private keys in emergency circumstances. These deployment issues are discussed in Appendix D.

Good Management Practices for Critical Information Asset Protection

To help you get started on security improvement, Appendix E contains a list of easy-to-implement low-cost or no-cost computer security measures. Below are additional, cross-cutting management practices that take into account the value of information and service provided by critical systems.

- *Know your interdependencies.* Keep track of who feeds information into your systems and by what means, and to whom you send information.
  - Alert managers of interdependent systems of events and incidents that may affect the quality of data they are sending or receiving from you.
  - Report security incidents to a central clearinghouse so that law enforcement authorities can determine whether a coordinated attack on multiple systems (often called "information warfare") is being attempted.
- *Improve internal incident reporting procedures*. Watch for patterns of intrusions or attempted intrusions.
- *Build redundancy into your system and procedures*.
  - Do more frequent backups and consider using more than one type of media. Test backup media regularly and frequently for recovery/restorability of files.
  - If continuity of service is part of criticality, consider maintaining a hot site or cold site as appropriate.
- *Arrange system architecture so that vulnerable networks or network segments can be quickly isolated or taken off line in the event of an attack.*
- *Institute a higher level of monitoring/intrusion detection for critical than noncritical systems* (e.g., more background auditing, more frequent analysis of usage patterns, lower thresholds for investigation of anomalies).

- *Rigorously screen personnel who have access to critical systems, especially those who may be involved in modification of architecture, operating systems, or hardware*. Consider granting access to source code based on citizenship and security clearances.
- *Use cryptography and strong authentication to protect information stored in files and databases in critical systems, as well as that transmitted over insecure channels, from corruption or theft.*

Chapter IV. Security Incident Planning[1]

Before the Worst Happens

Despite your best efforts to increase security awareness and to mitigate the risks arising from the constellation of threats and vulnerabilities affecting your system, it is likely that at some time you will experience a *computer security incident*—an adverse event that threatens some element of computer security: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. The definition of an incident will vary for each agency. However, the following categories and examples are generally applicable:

- *Compromise of integrity*, such as when a macro virus infects an application or a serious system vulnerability is discovered
- *Denial of service*, such as when an attacker has disabled a system or a worm has saturated network bandwidth
- *Misuse*, such as when an intruder (or insider) makes unauthorized use of an account
- *Damage*, such as when a virus destroys data
- *Intrusions*, such as when an intruder penetrates system security
- *Alterations*, such as when data is changed to effect system performance

Before a security incident occurs, you will want to develop a *computer security incident response capability* (CSIRC)—a set of policies and procedures defining security incidents and governing the actions to be taken when they occur. The CSIRC should include assignments of responsibilities, training, and awareness.

Establishing A Computer Security Incident Response Capability (CSIRC)

A CSIRC should be thought of as a direct extension of the contingency planning process. An agency's CSIRC should be the central capability for dealing with virtually any computer security problem that occurs: it should provide a means for reporting incidents, disseminating important incident-related information to management and users, and coordinating incident handling.

The goal of a CSIRC is to mitigate the potentially serious effects of a computer security-related problem. To achieve this aim, a CSIRC effort requires the involvement and cooperation of the entire agency. While the core of a CSIRC organization will be relatively small—perhaps five or fewer individuals—the CSIRC effort should involve the entire agency's management structures, communications and reporting mechanisms, and users. The specific objectives of an agency's

[1] Material in this chapter is drawn from the U.S. Department of Commerce, National Institute of Standards and Technology, *Establishing a Computer Security Incident Response Capability (CSIRC)*, NIST Special Publication 800-3 (Washington, D.C.: November 1991), which is available online at http://csrc.nist.gov/nistpubs/ .

CSIRC, which will influence its size and makeup, should include the following to the extent practicable:

- Facilitating centralized reporting of incidents
- Coordinating responses to incidents of a certain type or affecting a certain technology
- Providing direct technical assistance as needed
- Performing training and raising security awareness of users and vendors
- Providing a clearinghouse for relevant computer security information
- Promoting computer security policies within a constituency
- Developing or distributing software tools to the constituency
- Encouraging vendors to respond to product-related problems
- Acting as liaison to legal and criminal investigation authorities

CSIRC objectives should be simple, unambiguous, and realistic. For example, attempting to serve disparate constituencies, such as mainframe and microcomputer users, may be impractical, depending on fiscal constraints. When setting up a CSIRC, guard against adopting overly ambitious objectives at the outset.

Developing Communications Channels and Information Resources

The CSIRC needs to let users know how to contact it in case of emergencies and actual or suspected security breaches. It may be practical to maintain a "hotline" telephone number for urgent calls.

The CSIRC also needs a mechanism for alerting users to security threats, such as new viruses spread by Internet email or would-be intruders posing as technicians. Email bulletins pointing to an electronic information repository (usually on an agency intranet) can be used to make security information available in a format that is convenient for users and efficient for the CSIRC. Users can peruse and download information without assistance from the CSIRC personnel, enabling them to concentrate on incident handling and information gathering. An information repository should include the following items:

- Archived vulnerability or alert information
- Descriptions of the CSIRC and related information
- Agency security policies
- Reporting forms
- Procedures for reporting suspected problems or incidents
- Procedures for installing patches
- Self-help information, such as how to use access controls to improve integrity
- Information about current threats, such as viruses or software vulnerabilities

The CSIRC will also need to retain a variety of information for its own operational use and for conducting reviews of effectiveness and accountability, including contact information, activity logs, and incident logs.

Handling A Security Incident

When first notified of an incident, the CSIRC should follow an established set of procedures to verify the occurrence of the incident and notify users within and outside the agency who may be affected. If the source of the incident information is unfamiliar or not trusted, verify the source. Investigate the incident, at first hand if possible, to ensure that it is not a misunderstanding or hoax. Once the incident is verified, determine its scope. While the real scope of the incident may not be apparent at this stage, knowing whether it affects other agencies or organizations will determine who should be notified (e.g., senior management, legal department, Inspector General) and whether investigative agencies should be contacted.

After an incident has been resolved, conduct a *post mortem* examination so that the CSIRC can learn from the experience and, if necessary, update its procedures. The following types of incident information should be gathered, examined, and retained for future reference:

- How the incident started: which vulnerabilities were exploited, how access was gained, and other relevant details
- How the CSIRC became aware of the incident
- How the incident was resolved
- Whether existing procedures were adequate or require updating
- Whether vulnerabilities still need to be remediated
- Whether new contacts were made and whether additional contacts need to be made

For additional information, a bibliography of documents dealing with computer incident handling can be found at: http://www.cert.dfn.de/eng/pre99papers/certbib.html/

(this page purposely left blank)

Glossary

Definitions

Access	Opportunity to make use of an information system (IS) resource.
Access control	Limiting access to information system resources to authorized users, programs, processes, or other systems only.
Accountability	Principle that responsibilities for ownership and/or oversight of IS resources are explicitly assigned and that assignees are answerable to proper authorities for stewardship of resources under their control.
Agency	Federal department, major organizational unit within a department, or independent agency.
Alert	Notice of specific attack directed at an organization's IS resources.
Application	A software package designed to perform a specific set of functions, such as word processing or communications. See also **program**.
Attack	Intentional attempt to bypass the physical or information security measures and controls protecting an IS. Synonymous with **penetration**.
Attack signature	Activities or alterations to an IS indicating an attack or attempted attack, detectable by examination of audit trail logs.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established security policies and procedures, and/or to recommend necessary changes in controls, policies, or procedures to meet security objectives.
Audit trail	Chronological record of system activities or message routing that permits reconstruction and examination of a sequence of events.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator; or as a means of verifying a user's authorization to access specific types of information.
Authorization	Access privileges granted to a user, program, or process.
Availability	Timely, reliable access to data and information services for authorized users.
Back door	See **trap door**.
Backup	Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

Bandwidth	The amount of data that can be transmitted in a unit of time; for digital devices, bandwidth is usually expressed in bits or bytes per second.
Banner	Display on an IS that sets forth conditions and restrictions on system and/or data use.
Biometrics	Automated methods of authenticating or verifying a user based on physical or behavioral characteristics.
Bridge	A device that connects two networks or network segments; similar to a router but protocol-independent. See also **router**.
Browser	An application with a graphical user interface (GUI) that allows a user to access information on the World Wide Web.
Certificate	Digital record holding security information about a user (generally, the user's public key for data encryption).
Certification authority (CA)	A body responsible for authenticating that the information in a digital user certificate (e.g., a public key for data encryption) is bound to the owner of the certificate.
Change control	See **configuration management**.
Checksum	A value automatically computed on data to detect error or manipulation during transmission.
Cipher	An algorithm for encryption and decryption in which arbitrary symbols or groups of symbols are used to represent plain text, or in which units of plain text are rearranged, or both.
Classified information	Information that has been determined under an applicable authority—such as Executive Order 12958 or the Atomic Energy Act of 1954, as amended—to require protection against unauthorized disclosure to protect national security and that is marked to indicate its classification.
Client-server architecture	An architecture consisting of server programs that await and fulfill requests from client programs on the same or another computer.
Code	In computer programming, a set of symbols used to represent characters and format commands and instructions in a program. **Source code** refers to the set of commands and instructions making up a program.
Cold site	An alternate site with necessary electrical and communications connections and computer equipment, but no running system, maintained by an organization to facilitate prompt resumption of service after a disaster. See also **hot site**.
Compromise	A breach of security policy involving unauthorized disclosure; modification; destruction; or loss of information, whether deliberate or unintentional.

Computer	A machine that can be programmed in code to execute a set of instructions (program). In an IS, the term "computer" usually refers to the components inside the case: the motherboard, memory chips, and internal storage disk(s).
Computer network	A set of computers that are connected and able to exchange data.
Computer security	Measures and controls that ensure confidentiality, integrity, and availability of IS assets, including hardware, software, firmware, and information being processed, stored, and communicated. Synonymous with **information systems security**.
Concept of operations (CONOP)	Document detailing the method, act, process, or effect of using an IS.
Confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices.
Configuration control	Process of controlling modifications to hardware, software, firmware, and documentation to ensure that an IS is protected against improper modification before, during, and after system implementation.
Configuration management	Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IS.
Contingency plan	Plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, to ensure availability of critical resources and facilitate the continuity of operations in an emergency.
Critical asset	An asset that supports national security, national economic security, and/or crucial public health and safety activities.
Critical infrastructure	"Physical or cyber-based system essential to the minimum operations of the economy and government."(PDD-63 definition)
Cryptography	Science of encrypting plain data and information into a form intelligible only to authorized persons who are able to decrypt it.
Data integrity	A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
Denial of service	Result of any action or series of actions that prevent any part of an IS from providing data or other services to authorized users.
Dictionary attack	An attempt to gain access to an IS by guessing a user's password, using software that systematically enters words in a dictionary as passwords until a match is found. See also **password cracker**.
Digital signature	Cryptographic process used to assure the authenticity and nonrepudiation of a message originator and/or the integrity of a message.

Disaster recovery	The process of restoring an IS to full operation after an interruption in service, including equipment repair/replacement, file recovery/restoration, and resumption of service to users.
Email	Abbreviation for electronic mail, which consists of messages sent over an IS by communications applications. Email that is sent from one computer system to another or over the Internet must pass through gateways both to leave the originating system and to enter the receiving system.
Environment	Aggregate of the external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.
Event	An occurrence, not yet assessed, that may affect the performance of an IS. See **incident**.
Extranet	An **intranet** (q.v.) that is accessible or partially accessible to authorized users outside the organization.
Firewall	An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client-server architecture, used to protect internal networks or network segments from unauthorized users or processes.
Firmware	Application recorded in permanent or semipermanent computer memory.
Gateway	Interface between networks that facilitates compatibility by adapting transmission speeds, protocols, codes, or security measures.
Hacker	Any unauthorized user who gains, or attempts to gain, access to an IS, regardless of motivation.
Hardware	The physical components of a computer system.
Hijacking	An attack that occurs during an authenticated session with a database or system. The attacker disables a user's desktop system, intercepts responses from the application, and responds in ways that prolong the session. See also **spoofing**.
Hot site	An alternate site with a duplicate IS already set up and running, maintained by an organization or its contractor to ensure continuity of service for critical systems in the event of a disaster. See also **cold site**.
Identification	The process used by an IS to recognize an entity such as a user or another process.
Incident	An occurrence that has been assessed as having an adverse effect on the security or performance of an IS.
Information operations (IO)	Actions taken to affect an adversary's information and information systems while defending one's own information and information systems.

Information system (IS)	All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS may be automated (e.g., a computerized information system) or manual (e.g., a library's card catalog).
Information systems security	See **computer security**.
Information warfare (IW)	IO conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.
Integrity	Condition existing when an IS operates without unauthorized modification, alteration, impairment, or destruction of any of its components.
Interface	A common boundary or connector between two applications or devices, such as the graphical user interface (GUI) that allows a human user to interact with an application written in code.
Internet	A decentralized, global network of computers (Internet hosts), linked by the use of common communications protocols (Transmission Control Protocol/Internet protocol, or TCP/IP). The Internet allows users worldwide to exchange messages, data, and images. See **World Wide Web**.
Internet protocol (IP)	A communications protocol that routes packets of data. The address of the destination system is used by intermediate routers to select a path through the network. See also **Transmission Control Protocol (TCP)**.
Intranet	A private network for communications and sharing of information that, like the Internet, is based on TCP/IP but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall. See also **extranet**.
Intrusion	Attacks or attempted attacks from outside the security perimeter of an IS.
Laptop computer	A portable computer usually powered by a rechargeable battery. The smaller versions are also called notebook computers.
Logic bomb	A small, malicious program that is activated by a trigger (such as a date or the number of times a file is accessed), usually to destroy data or source code. See **virus**.
Malicious program	Source code incorporated into an application that directs an IS to perform an unauthorized, often destructive, action.
Media	Short for storage media: physical objects on which data can be stored, such as hard disks, CD-ROMs, floppy disks, and tape.

Memory	A computer's internal capacity to store data, determined by the microchips installed.
Modem	Acronym for *mo*dulator-*dem*odulator. A device or application that permit a computer to transmit data over telephone lines by converting digital data to an analog signal.
Network security	Security procedures and controls that protect a network from: (1) unauthorized access, modification, and information disclosure; and (2) physical impairment or destruction.
Network topology	The architectural layout of a network. Common topologies include bus (nodes connected to a single backbone cable), ring (nodes connected serially in a closed loop), and star (nodes connected to a central hub). See also **network**.
Nonrepudiation	A cryptographic service that legally prevents the originator of a message from denying authorship at a later date.
Operating system	Software required by every computer that: (1) enables it to perform basic tasks such as controlling disks, drives, and peripheral devices; and (2) provides a platform on which applications can run.
Optical scanner	A peripheral device that can read printed text or illustrations and translate them into a digitized image (bit map) that can be stored, displayed, and manipulated on a computer.
Packet	A piece of a message, usually containing the destination address, transmitted over a network by communications software.
Packet filter	A type of firewall that examines each packet and accepts or rejects it based on the security policy programmed into it in the form of rules.
Password	A string of characters containing letters, numbers, and other keyboard symbols that is used to authenticate a user's identity or authorize access to data. A password is generally known only to the authorized user who originated it.
Password cracker	An application that tests for passwords that can be easily guessed, such as words in the dictionary or simple strings of characters (e.g., "abcdefgh" or "qwertyuiop").
Patch	A modification to software that fixes an error in an application already installed on an IS, generally supplied by the vendor of the software.
Penetration	See **attack**.
Peripheral equipment	Any external device attached to a computer, including monitors, keyboards, mice, printers, optical scanners, and the like.
Probe	A device programmed to gather information about an IS or its users.

Program	A set of instructions in code that, when executed, causes a computer to perform a task.
Protocol	A set of rules and formats, semantic and syntactic, that allow one IS to exchange information with another.
Proxy	An application or device acting on behalf of another in responding to protocol requests.
Proxy server	A server that runs a proxy version of an application, such as email, and filters messages according to a set of rules for that application.
Purge	To render stored applications, files, and other information on a system unrecoverable. See also **sanitize**.
Push technology	Technology that allows users to sign up for automatic downloads of online content, such as virus signature file updates, patches, news, and Web site updates, to their email boxes or other designated directories on their computers.
Redundancy	Duplication of system components (e.g., hard drives), information (e.g., backup tapes, archived files), or personnel intended to increase the reliability of service and/or decrease the risk of information loss.
Remote access	Use of a modem and communications software to connect to a computer network from a distant location via a telephone line or wireless connection.
Risk management	The identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected.
Risk-based management	Risk management that considers unquantifiable, speculative events as well as probabilistic events (that is, uncertainty as well as risk).
Router	A device that connects two networks or network segments and may use IP to route messages. See also **bridge**.
Sanitize	To expunge data from storage media (e.g., diskettes, CD-ROMs, tapes) so that data recovery is impossible. See also **purge**.
Secure Hash Algorithm	Algorithm that can generate a condensed message representation called a message digest.
Sensitive information	Unclassified information, the loss, misuse, or unauthorized disclosure or modification of which could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals protected by the Privacy Act (5 U.S.C. Section 552a). Information systems containing sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235).

Server	A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.
Sniffer	A software tool for monitoring network traffic. On a TCP/IP network, sniffers audit information packets.
Software	The electronically stored commands and instructions that make an IS functional, including the operating system, applications, and communications protocols.
Source code	See **code**.
Spoofing	Unauthorized use of legitimate identification and authentication data, such as user IDs and passwords, by an intruder to impersonate an authorized user or process to gain access to an IS or data on it.
Superuser	A user who is authorized to modify and control IS processes, devices, networks, and file systems.
System administrator (SA)	Person responsible for the effective operation and maintenance of an IS, including implementation of standard procedures and controls to enforce an organization's security policy.
System integrity	Optimal functioning of an IS, free from unauthorized impairment or manipulation.
System security officer	Person assigned to implement an organization's computer security policy. Also referred to as a **system security program manager**.
System security plan	A formal document listing the tasks necessary to meet system security requirements, a schedule for their accomplishments, and to whom responsibilities for each task are assigned.
Telecommunications	Preparation, transmission, communication, or related processing of information (text, images, sounds, or other data) by electrical, electromagnetic, or similar means.
Threat	Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment.
Time bomb	See **logic bomb**. A time bomb is a type of logic bomb that is triggered by the arrival of a date or time.
Transmission Control Protocol (TCP)	A protocol that establishes a connection and provides a reliable transport service between source and destination systems. TCP calls IP to provide a routing service. See **Internet protocol (IP)**.
Trap door	Hidden code or hardware device used to circumvent security controls. Synonymous with **back door**.

Trojan horse	A malicious program such as a virus or a worm, hidden in an innocent-looking piece of software, usually for the purpose of unauthorized collection, alteration, or destruction of information.
Tunneling	A method for circumventing a firewall by hiding a message that would be rejected by the firewall inside a second, acceptable message.
User	A person or process authorized to access an IS.
User ID	Unique symbol or character string used by an IS to recognize a specific user.
Utility	A program that performs a specific task for an IS, such as managing a disk drive or printer.
Virus	A small, self-replicating, malicious program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A **file virus** executes when an infected file is accessed. A **macro virus** infects the executable code embedded in Microsoft® Office® programs that allows users to generate macros.
Virus signature	Alterations to files or applications indicating the presence of a virus, detectable by virus scanning software.
Vulnerability	A flaw in security procedures, software, internal system controls, or implementation of an IS that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.
Vulnerability assessment	An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to: (1) identify weaknesses that could be exploited; and (2) predict the effectiveness of additional security measures in protecting information resources from attack.
Vulnerability audit	The process of identifying and documenting specific vulnerabilities in critical information systems.
Web site	A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages. See **World Wide Web**.
World Wide Web (WWW, Web)	A system of Internet hosts that support documents formatted in HTML (*H*yper*T*ext *M*arkup *L*anguage), which contain links to other documents (hyperlinks), and to audio, video, and graphics images. Users can access the Web with special applications called browsers, such as Netscape® Navigator® and Microsoft® Internet Explorer®.
Worm	A small, malicious program similar to a virus, except that it cannot self-replicate. See **virus**.

Acronyms

AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CONOP	Concept of operations
DES	Data Encryption Standard
FAQs	Frequently asked questions
GUI	Graphical user interface
IS	Information system
IT	Information technology
LAN	Local area network
PC	Personal computer
SBU	Sensitive but unclassified
SHA	Secure Hash Algorithm
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Universal (or Uniform) Resource Locator; refers to the address of a World Wide Web site
WAN	Wide area network
WWW	World Wide Web

Appendix A. Bibliography and Additional Sources of Security Information

Bibliography of Sources Consulted

Alexander, Michael. *The Underground Guide to Computer Security*. Reading, Mass.: Addison-Wesley. 1996.

Amoroso, Edward G. *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response*. Sparta, N.J.: Intrusion.Net Books. 1999.

Bace, Rebecca. *An Introduction to Intrusion Detection and Assessment*. Prepared for ICSA.net. Available online for download at http://www.icsa.net/html/communities/ids/White%20paper/index.shtml (*Note*: document requires Adobe® Acrobat® Reader).

Board of Governors of the Federal Reserve System. "Sound Practices Guidance for Information Security for Networks." Federal Reserve Board Supervision and Regulation Letter SR 97-32 (SUP). September 1997. Available online at http://www.bog.frb.fed.us/boarddocs/SRLETTERS/1997.

Booz-Allen & Hamilton, Inc. *Infrastructure Asset Evaluation Survey*. Developed for the U.S. Critical Infrastructure Assurance Office (CIAO) under contract number 40AAEX909180. November 1999.

Canadian Communications Security Establishment. "Government of Canada Firewall Frequently Asked Questions." Available online at http://www.cse-cst.gc.ca/cse/english/faq/firewall.html.

Executive Office of the President. *Defending America's Cyberspace: National Plan for Information Systems Protection*. Version 1.0. November 1999.

Executive Office of the President. *Protecting America's Critical Infrastructures*. Presidential Decision Directive/NSC-63. May 22, 1998. Available online at http://www.ciao.gov/CIAO_Document_Library/paper598.html

KPMG Peat Marwick LLP. *Vulnerability Assessment Framework 1.1*. Developed under contract to the CIAO, October 1998.

Krause, Micki and Harold F. Tipton, eds. *Handbook of Information Security Management 1999*. Boca Raton: Auerbach. 1999.

Network Associates, Inc. *An Introduction to Computer Viruses (and Other Destructive Programs)*. McAfee White Paper. Available online at http://www.nai.com/asp_set/anti_virus/library/white_papers.asp. (*Note*: there are underscores between "asp" and "set," "anti" and "virus," and "white" and "papers" in the URL.)

U.S. Department of Commerce. National Institute of Standards and Technology. *Establishing a Computer Security Incident Response Capability (CSIRC)*. NIST Special Publication 800-3. Washington, D.C. November 1991. Available online at http://csrc.nist.gov/nistpubs/ .

U.S. Department of Commerce. National Institute of Standards and Technology. *Guide for Developing Security Plans for Information Technology Systems.* NIST Special Publication 800-18. Washington, D.C. December 1998. Available online at http://csrc.nist.gov/nistpubs/ .

U.S. Department of Commerce. National Institute of Standards and Technology. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. NIST Special Publication 800-16. Washington, D.C. April 1998. Available online at http://csrc.nist.gov/nistpubs/ .

U.S. Department of Education. National Center for Education Statistics. *Safeguarding Your Technology*. NCES Publication No. 98297. Washington, D.C. September 1998. Available online at http://nces.ed.gov/pubs98/safetech.

Additional Sources of Security Information

NASA Automated Systems Incident Response Capability (NASIRC) 95

http://www-nasirc.nasa.gov/

The NASIRC was created to assist NASA in complying with OMB Circular A-130, the Computer Security Act of 1987, and a range of other Federal policies, laws, and regulations pertaining to unclassified and classified information technology security. NASIRC provides security management, analysis, and technical support for the establishment of an agencywide computer network systems incident response and coordination capability.

The NASIRC Web site references the software-patch-containing Web sites of most major vendors and the Web sites of other security organizations.

National Institute Of Standards and Technology (NIST) Computer Security Resource Clearinghouse

http://csrc.nist.gov

The Computer Security Resource Clearinghouse (CSRC) is designed to collect and disseminate computer security information and resources to help users, systems administrators, managers, and security professionals better protect their data and systems. A primary goal of the CSRC is to raise awareness of all computer systems users, from novice to expert, about computer security.

The following types of information are available at the CSRC Web site:

- *Topics*. Information on various computer security subjects, including current NIST information technology (IT) security programs and projects. Topics are authentication,

common criteria, emerging technologies, encryption and keys, incident handling, security objects, testing, and virus information.

- *Calendar of Events*. Security-related seminars and conferences.
- *Organizations*. Security-related organizations.
- *Policies*. Current U.S. Government policy documents and sample policy documents.
- *Publications*. Recent publications from a variety of sources that deal with information security issues.
- *Training*. Resources for the computer security professional or trainer.

The Federal Computer Incident Response Capability (FEDCIRC)

http://www.fedcirc.gov/

FEDCIRC provides a central focal point for incident reporting, handling, prevention, and recognition.

The FEDCIRC Web site provides information on the following security-related areas:

- Tools for network monitoring, password cracking, and vulnerability assessment
- Antivirus software and measures
- Intrusion detection
- Vendor patches and updates

The Computer Emergency Response Team (CERT®) Coordination Center

http://www.cert.org/

The CERT Coordination Center is part of the Survivable Systems Initiative at the Software Engineering Institute, a Federally funded research and development program established in 1988 at Carnegie Mellon University. The CERT Coordination Center studies Internet security vulnerabilities, provides incident response services, publishes security alerts and system security improvement information, and researches security and survivability in wide area network computing.

The CERT Coordination Center Web site contains a wide variety of security improvement information, including the following:

- Sound practices for detecting and responding to intrusions
- Sound practices for recovering from intrusions
- A list of virus databases
- Virus organizations and papers
- Antivirus software vendors
- Training information

Defense Information Systems Agency

http://www.disa.mil

The Defense Information System Agency (DISA) is the Department of Defense's lead organization for information security. The site includes IASE, a Web-based help environment for information assurance available to anyone with a .gov or .mil user account.

Air Force Computer Emergency Response Team (AFCERT)

http://afcert.csap.af.mil/

The mission of the AFCERT is to provide information protection assistance to Air Force units.

The AFCERT Web site has links to other sites that provide information in the following areas:

- Virus response
- Intrusion detection
- Incident response
- Deploying firewalls
- Firewall product overview
- Authentication and encryption

The Canadian Communications Security Establishment (CSE)

http://www.cse-cst.gc.ca/cse/english/faq/firewall.html

The CSE is the lead agency that delivers information technology security solutions to the Government of Canada.

The Canadian CSE Web site contains useful information about the following topics:

- Firewall architectures
- Firewall functionality
- Firewall selection
- Firewall installation and configuration

Board of Governors of the Federal Reserve System

http://www.bog.frb.fed.us/boarddocs/SRLETTERS/1997/sr9732a1.pdf

In 1996, the Federal Reserve Bank of New York formed a team to benchmark sound information security policies and practices. The team interviewed a cross-section of financial service institutions as well as security firms, service providers, common carriers, CPA firms, and other banking industry-related organizations. In 1997, the Board of Governors of the Federal Reserve System issued "Sound Practices Guidance For Information Security for Networks," which reported on the information gathered in that survey.

The report contains a wealth of useful information on sound practices in the following areas:

- Risk management practices
- Security policy development
- Network security and monitoring
- Access control
- Confidentiality
- Configuration control
- Personnel
- Business continuity

ICSA.net Intrusion Detection Paper

http://www.icsa.net/html/communities/ids/White%20paper/index.shtml (*Note*: document requires Adobe® Acrobat® Reader).

ICSA.net is a private company that provides security assurance services. ICSA.net formed an Intrusion Detection Systems Consortium to work toward common goals. This consortium published *An Introduction to Intrusion Detection and Assessment*, a report prepared by Rebecca Bace of Infidel, Inc., which contains useful information about intrusion detection systems.

General Accounting Office (GAO)

http://www.gao.gov/special.pubs/ai99139.pdf

The Accounting and Information Management Division of the General Accounting Office has published *Information Security Risk Assessment- Practices of Leading Organizations* (available at the Web site listed above) to help Federal managers implement an ongoing information security risk assessment process. It provides detailed case histories of practical risk assessment procedures adopted by four public and private organizations known for their efforts to implement good risk assessment procedures.

Critical Infrastructure Assurance Office (CIAO)

http://www.ciao.ncr.gov/

The CIAO's Web site contains the text of this guide and summary and full-text versions of PDD-63. The online version of the guide will be updated more frequently than the printed version, especially the links to computer security information sources.

Ron Rivest's Collection Of Links On Cryptography And Security

http://theory.lcs.mit.edu/~rivest/crypto-security.html

This Web site contains links to many useful Web sites dealing with cryptography and security, from one of the inventors of the widely used RSA algorithm for encrypting data.

Appendix B. Overview of Federal Computer Security and Information Resources Management (IRM) Policy

Historical and Legal Background

Introduction

During the past 15 years, both the Congress and the Executive Branch have enacted substantial legal and policy reforms to keep pace with technological change and innovation. This section briefly identifies major themes and authorities that support the development of Federal computer security and information resources management (IRM) responsibilities.

Historical Background: Fifty Years of Change

The Congress and the Executive Branch orchestrate the development of Federal computer security and IRM responsibilities through legislation and administrative requirements. Relevant law encompasses a wide range of issues, ranging from privacy and the implementation of standards to Government performance and concerns for national security. Figure B-1, *Federal Computer Security Authorities Timeline*, on the next page traces the development of Federal computer security policy from its inception.

Social, Political, and Legal Developments, 1932 - 1949

Many of the current legal developments in Federal Government computer security can be traced to a period ranging from President Roosevelt's New Deal to the onset of the Cold War, when information requests between government and other parties increased in reaction to the need for governmental services.[1] These political and social changes continue to significantly influence the debate today over standards and guidelines for computer security of Federal Government information technology (IT).

Three significant legal developments are worth noting. First, the Congress created the Office of Management and Budget, which has significant IRM oversight responsibility, in response to the need to manage information exchanges between the Government and the people.[2]

[1] See H.R. Rep. No. 927, 101st Cong., 2nd Sess. 1990, 1990 WL 201562 (Leg. Hist.); Paperwork Reduction and Federal Information Resources Management Act of 1990, House Report No. 101-927, October 23, 1990 [To accompany H.R. 3695].

[2] Congress passed the Federal Reports Act of 1942 to authorize the Bureau of the Budget (OMB's predecessor) "to coordinate Federal reporting services, to eliminate duplication and reduce the cost of such services, and to minimize the burdens of furnishing information to Federal agencies." The core of the current law's concern for reducing information collection burdens and improving the management of Federal information resources is found in this 52- year-old statutory mandate. In 1970, the former Bureau of the Budget was reconstituted as the Office of Management and Budget (OMB) in order to strengthen central management leadership and capacity in the Executive Branch.

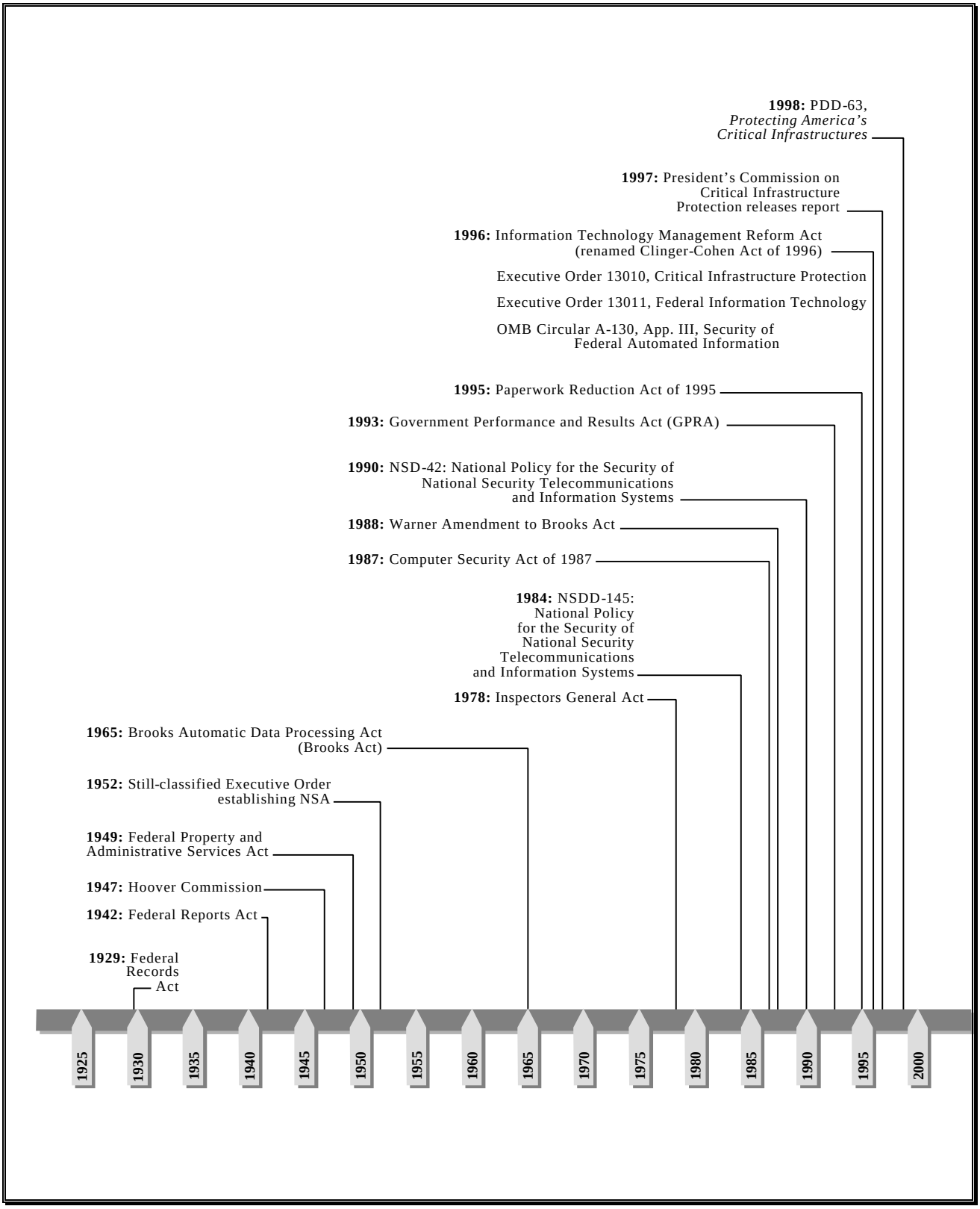

Figure B-1. Federal Computer Security Authorities Timeline

Second, the Congress established the General Services Administration in 1949 by passing the Federal Property and Administrative Services Act to centralize procurement responsibilities.[3] The Congress and the Executive Branch traditionally use the Federal Government's ability to link procurement to security; the GSA's contributions to Federal Government computer security are therefore quite significant.

Third, the Truman Administration's creation of the National Security Agency in 1952 laid the foundation for the emergence of a significant actor in the development of standards and guidelines.[4] NSA is well known for its focus on, and expertise in, creating mechanisms to protect access to classified materials. Current law restricts NSA's jurisdiction over the creation of computer security guidelines and standards to classified and national security systems only.

Centralized to Decentralized Government Management, 1949-1999

Congressional legislation during the past 35 years has wavered between centralized IRM and decentralized models recommending interagency cooperation for more complex matters. Passage of the Brooks Automatic Data Processing Act in 1965 (Brooks Act) further conferred upon GSA Governmentwide responsibility for the acquisition of IT. Congress repealed the Brooks Act with passage of the Information Technology Management Reform Act (renamed the Clinger-Cohen Act of 1996), requiring agencies to take responsibility for core business functions, including a wide range of computer security and information resource management requirements.

Critical Infrastructure Protection, 1996–1999

Today's political and IRM policy structure debate is by no means resolved. For the last several years, the Clinton Administration has carefully studied the Federal Government's growing dependencies on critical infrastructures, both internally and externally, with the private sector and state and local governments. In July 1996, the President's Commission on Critical Infrastructure Protection (PCCIP) was formed to advise and assist the President of the United States by recommending a national strategy for protecting and assuring critical infrastructures from physical and cyber threats. The President signed Presidential Decision Directive 63 (PDD-63) in May 1998, incorporating many of the PCCIP's recommendations.

Principal Themes

Three themes characterize Congressional, Executive Branch, and regulatory activity and thinking: (1) tensions between security and public access to information; (2) efficiency and Governmentwide information resources management; and (3) critical infrastructure protection.

[3] The Hoover Commission, headed by former President Herbert Hoover, was formed in 1947 to recommend to the President and Congress ways to improve administrative activities of the Federal Government. The Hoover Commission recommended establishing an independent "Office of General Services" that would assume the existing responsibilities of several entities, including the Treasury Department, the National Archives establishment, and the Federal Works Agency.

[4] The NSA was created by a still-classified Executive Order in 1952. Refer to Executive Order 12333 (*U.S. Intelligence Activities*) for the basic structure of the U.S. Intelligence Community. This Executive Order delineates the jurisdictional boundaries between the intelligence agencies and provides a legal basis of authority for their activities.

Tension: Security vs. Access to Data

The first core issue emerges from the development of standards and guidelines to improve the security of sensitive information in Federal computer systems and to open access to information held by the Government. This tension results from two competing necessities—the need to restrict access to certain, generally classified, information affecting national security; and the need to guarantee access to other types of data (e.g., consumer information) intended to be widely disseminated for public benefit.

President Reagan issued National Security Decision Directive 145 (NSDD-145) in response to the growing threat of foreign exploitation of computer-based information systems in the Government. Data deemed vulnerable by NSDD-145 included classified and certain other sensitive-but-unclassified (SBU) information remitted by Federal computers or telecommunications systems, including agricultural, industrial, and commercial data.[5] NSDD-145 assigned to the National Security Agency the responsibility for developing standards and guidelines to protect these types of data.

In response, Congress effectively rescinded NSDD-145 by expanding power in civilian government and restricting the NSA's authority to develop Federal standards and guidelines as a means of best resolving the tensions between security and access.

An Expanded Role for the National Institute of Standards and Technology (NIST): Sensitive but Unclassified Information. Congress feared that the Administration was seeking not simply to protect classified information, national security, and other unclassified information held by the Government, but also to control access to information in private sector systems. Congress subsequently passed the Computer Security Act of 1987, which replaced NSDD-145 as U.S. Government policy.

The Computer Security Act established a system for creating uniform standards and guidelines to protect information in Federal computer systems. NIST was given the responsibility of protecting the privacy of SBU information. NSA retained control of standards development covering all classified systems, but its role was limited by the Computer Security Act to providing technical assistance to NIST.[6]

In addition, Congress established the Computer Systems Security Privacy Advisory Board (CSSPAB) as a public advisory board in the Computer Security Act of 1987. The Board is composed of twelve members, in addition to the Chairperson, who are recognized experts in the fields of computer and telecommunications systems security and technology. The CSSPAB advises the Secretary of Commerce and the Director of NIST.

Warner Amendment: SBU National Security Systems. One year later, in 1988, Congress passed the Warner Amendment to the Brooks Act. This Amendment, which Congress linked to policies

[5] Computer Security Act of 1987, Legislative History, House Report No. 100-153 (II) (June 11, 1987); Cong. Record Vol. 133 (1987). NSDD-145 was issued in 1984.

[6] Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning Implementation of Public Law 100-235 [Computer Security Act] (March 1989).

covering procurement rules, defines certain specific types of SBU IT that must be treated as classified technology. The amendment thus carved out a limited area of jurisdiction for NSA over SBU IT.

The Warner Amendment generally covers the function, operation, or use of information technology in any of the following:

- Intelligence activities
- Cryptographic activities related to national security
- The direct command and control of military forces
- Equipment that is an integral part of a weapon or weapons system
- IT that is critical to military or intelligence missions

During Congressional debates covering the Paperwork Reduction Act, and later with passage of the Clinger-Cohen Act, Congress explicitly excluded from NIST and OMB the authority to create and manage standards development for Warner Amendment categories, defined as "national security systems." Certain other types of national security/emergency preparedness IT exclusions from OMB oversight responsibilities are more clearly defined below.[7]

National Security Directive 42 (NSD-42) and the National Security Telecommunications Information Systems Security Committee (NSTISSC). In July 1990, the Bush Administration, in direct compliance with the Computer Security Act, issued National Security Directive 42 (NSD-42)[8], which created the National Security Telecommunications Information Systems Security Committee (NSTISSC). The NSTISSC includes 21 departments and agencies from the civilian, intelligence, law enforcement, and defense communities. The NSTISSC provides a forum for discussion of policy issues and sets national policy. Through its issuance system, the NSTISSC also promulgates direction, operational procedures, and guidance for the security of national security systems.[9]

OMB Oversight and Circular A-130, Appendix. III. Law and policy covering standards development have not changed significantly since the Computer Security Act, with one exception. In the Paperwork Reduction Act, and subsequently in the Clinger-Cohen Act of 1996, Congress required OMB to take on greater responsibility for overseeing the development and management of Federal computer security issues. These responsibilities include the full range of IT concerns, such as privacy (public access to, and protection of, data held by the Government), vulnerability and risk assessments, and efficiency of Federal Government and private sector information exchanges.

---

[7] See, for example, OMB Circular A-130, App. III, Security of Federal Automated Information Systems (February 1986) at Section 4(b) (excluding national security emergency preparedness activities conducted in accordance with Executive Order 12472).

[8] *National Policy for the Security of National Security Telecommunications and Information Systems* (supersedes NSDD-145).

[9] See, e.g., NSTISSD No. 503, *Incident Response and Vulnerability Reporting for National Security Systems* (August 30, 1993), which establishes the National Security Information Systems Incident Reporting Program (NSISIP); see also NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary (June 5, 1992).

Efficiency and Governmentwide Information Management

The second core issue incorporates several IRM themes, including: (1) Government efforts to improve performance and results in use of IT; (2) reducing the burden of information collection on the public and maximizing the use of information collected from the public; and (3) constructing a Governmentwide IRM model that allows for both decentralized decision making and responsibility *and* multiple-agency coordination of such IRM areas as large procurements, research and development, and budget efforts.

Many of these IRM challenges have been debated in Congress and the Administration throughout the 1990s and are incorporated into three legislative authorities: the Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, and the Government Performance and Results Act of 1993 (GPRA). President Clinton required implementation of these laws in Executive Order 13011, *Federal Information Technology*.

Improving Performance and Results. To improve the efficiency and effectiveness of Federal programs, Congress passed the Government Performance and Results Act of 1993 (GPRA). GPRA established a system to set goals for program performance and to measure results. OMB was charged with implementing GPRA, which includes IRM programs and practices. Clinger-Cohen and Executive Order 13011 both mandate that agencies set goals, measure performance, and report on progress to improve efficiency and effectiveness of operations through the use of IT.[10]

Reducing the Burden, Increasing Efficiency. The Paperwork Reduction Act of 1995[11] is one of the most significant legislative initiatives affecting Governmentwide IRM practices. The Act's roots can be traced to the exponential growth in paperwork caused by the proliferation of New Deal agencies and missions at the onset of World Was II.[12]

The Paperwork Reduction Act addresses concerns over appropriate dissemination and collection of information between the Government and the public. It also:

- Directs all Federal agencies to obtain OMB review and approval of plans to collect information from the public and industry.
- Requires Federal agencies to give the public and industry an opportunity to participate in the agency review process for each proposed information collection effort by providing an opportunity to comment before submission to OMB.

[10] *Executive Guide: Effectively Implementing the Government Performance and Results Act*, United States General Accounting Office, Comptroller of the United States (June 1996), GAO/GGD-96-118.

[11] Paperwork Reduction Act of 1995 (P.L. 104-13). For an excellent background history on the Paperwork Reduction Act of 1995, review the legislative history.

[12] Paperwork Reduction and Federal Information Resources Management Act of 1990, House Report No. 101-927 (October 23, 1990) (Discussion and Background Section). Congress initially addressed reducing the burden of Government demands on the public through the Federal Records Act, which created the Management and Budget Office in 1929. Congress further centralized management of paperwork collection and dissemination in the Paperwork Collection Act of 1980, which granted OMB authority to judge whether agency activities were necessary.

- Improves the quality and use of Federal information, through the use of IT and measures to minimize the human effort and financial costs (burden) necessary to provide the information to meet Federal agency requirements.

The Paperwork Reduction Act reaffirmed the system of managing IT established by the Computer Security Act of 1987; to wit, NIST is charged with development of computer security standards and guidelines covering SBU IT and NSA retains authority for standards development covering classified IT. However, Congress also underscored the importance of the Warner Amendment limitations by *restricting* OMB's jurisdiction to management of a limited class of SBU IT, or "national security systems." Thus, management of classified and specifically identified SBU IT for national security systems remain outside the scope of OMB's jurisdiction.[13]

Governmentwide IRM Management: OMB. Congress took further steps to consolidate OMB's significant role in managing Federal computer security and IRM responsibilities in passing the Information Technology Management Reform Act of 1996 (renamed the Clinger-Cohen Act). Congress, in passing the Clinger-Cohen Act, reversed three decades of enforcing minimum computer security requirements through centralized procurement authority.

Specifically, the Clinger-Cohen Act repealed Section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759) and the Brooks Act, eliminating the General Services Administration's exclusive authority to acquire computer resources for all of the Federal Government. The Clinger-Cohen Act assigns overall responsibility for the acquisition and management of IT, previously referred to as Federal Information Processing (FIP), in the Federal Government to the Director, Office of Management and Budget (OMB). Although the Brooks Act was repealed, Congress incorporated the Warner Amendment restrictions directly into the Clinger-Cohen Act.[14]

Highlights of the Clinger-Cohen Act are listed in the box on the next page.

[13] Paperwork Reduction Act of 1995 Legislative History (Coordination of Federal Information Policy, Section 2).
[14] See 10 U.S.C. Section 2315(a) (Warner Amendment).

Clinger-Cohen Act of 1996

The Clinger-Cohen Act gives the authority to acquire information technology (IT) resources to the head of each executive agency and makes each responsible for effectively managing agency IT investments. The primary purposes of the Act are to streamline IT acquisitions and emphasize life-cycle management of IT as a capital investment.[15] The key acquisition actions are to:

- Give IT procurement authority back to the agencies.
- Eliminate the Federal Information Resources Management Regulation (FIRMR) which governed acquisition and management of FIP (computer and telecommunications) resources.
- Move the General Services Board of Contract Appeals authority to hear bid protests on IT contracts to the General Accounting Office (GAO).
- Encourage incremental acquisition of IT systems.
- Encourage the acquisition of commercial-off-the-shelf (COTS) IT products.
- Allow the Administrator for Federal Procurement Policy to conduct pilot programs in Federal agencies to test alternative approaches for acquisition of IT resources.

The key IT management actions are to require agency heads to:

- Design and implement an IT management process for maximizing the value and assessing and managing the risks of the IT acquisitions.
- Integrate the IT management process with the processes for making budget, financial, and program management decisions.
- Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of IT, and prepare an annual report, to be included in the executive agency's budget submission to Congress, on the progress in achieving the goals.
- Ensure that the agency sets performance measurements that accurately assess how well the IT supports agency programs.
- Ensure that the information security policies, procedures, and practices of the agency are adequate.
- Appoint a Chief Information Officer (CIO).
- Inventory all computer equipment and maintain an inventory of any such equipment that is excess or surplus property.

On July 16, 1996, President Clinton issued Executive Order 13011, creating the CIO Council and directing Executive Branch agencies to implement each of the laws discussed in this section. The Executive Order requires agencies to:

- Significantly improve the management of their information systems.
- Refocus IT management to support directly their strategic missions.

[15] See also Chief Information Officer Web site materials at http://www.cio.gov/docs/exo13011.html/.

- Establish clear accountability for information resources management activities.
- Cooperate in the use of IT to improve the productivity of Federal programs.
- Establish an interagency support structure, the CIO Council.

OMB Circular A-130, *Management of Federal Resources*, specifically Appendix III, Security of Federal Automated Information Resources, is the principal administrative vehicle for implementing these IRM laws and polices. A-130, which was initially written in 1985, sets out Federal agency requirements for adhering to information security standards developed by NIST in accordance with the Computer Security Act. In 1996, A-130 was specifically designed to place responsibility for information security with the individual agency Chief Information Officers (CIOs). The enforcement of A-130 requires the reporting of "material weaknesses" in information security through an OMB budgetary review process.

Critical Infrastructure Protection

After the bombing of the Murrah Federal Building in Oklahoma City in 1995, the Attorney General formed a working group to address physical and, for the first time, cyber threats to the nation's critical infrastructure facilities. The Critical Infrastructure Working Group (CIWG) reviewed the history of IRM, as well as laws and policies covering terrorism, law enforcement, and national security.[16] The CIWG concluded that there were both civilian and government infrastructures critical to the security of the nation and that further analysis was needed to lay out a long-term strategy for understanding threats, vulnerabilities, and interdependencies.

President's Commission on Critical Infrastructure Protection (PCCIP): Critical Foundations. In January 1996, the CIWG recommended that an Executive Order be issued to create a President's Commission on Critical Infrastructure Protection to further analyze long-term solutions.[17] The PCCIP, which included commissioners from both government and the private sector, studied shared dependencies on critical infrastructure systems within government, and those shared with the private sector. The PCCIP agenda highlighted the impact and development of computer technologies, which affect all aspects of American commerce and society, including national security.

The Commission's recommendations for further action included the following:

- Establishing new programs to develop national infrastructure protection
- Partnering with the private sector and engaging industry cooperation
- Developing new governmental structures to achieve these goals

Based on its findings, the PCCIP issued an extensive report, *Critical Foundations: Protecting America's Infrastructures*, in October 1997.

[16] The CIWG also studied threats to the nation's critical infrastructures from the perspectives of two additional parties—private sector owners and operators of critical infrastructures, and state and local partners, who include "first responders" in emergencies.

[17] Executive Order 13010, *Critical Infrastructure Protection* (July 1996); see Critical Infrastructure Working Group report January 1996. See also Critical Infrastructure Working Group report (January 1996) (FOUO).

Presidential Decision Directive 63 (PDD-63) and the National Plan: Prioritizing IRM Programs. Findings from the PCCIP report were subsequently incorporated into PDD-63, *Protecting America's Critical Infrastructures*, issued May 22, 1998. These programmatic and policy objectives receive further elaboration in *Defending America's Cyberspace: National Plan for the Information Systems Protection*.

Statutory and Regulatory Authorities and Executive Branch Policy Guidance Applicable to the Protection of Critical Infrastructures

Statutes

- Computer Fraud and Abuse Act of 1986, P.L. 99-474, 18 U.S.C. 1030
- Computer Security Act of 1987, P.L. 100-235, 40 U.S.C. 759
- Defense Production Act of 1950, as amended, P.L. 102-590, November 10, 1992
- Electronic Communications Privacy Act of 1986, P.L. 99-508
- Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. 1352
- Freedom of Information Act of 1974, 5 U.S.C. 552
- Government Performance and Results Act of 1993, P.L. 103-62
- Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), Division E of P.L. 104-106, 40 USC 1401, February 10, 1996
- Paperwork Reduction Act of 1978, as amended, P.L. 104-13, 109 Stat 163, 44 U.S.C. Ch 35
- Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (e) (10)
- Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288

Executive Office of the President

- Executive Order (EO) 10421, *Providing for the Physical Security of Facilities Important to the National Defense*
- EO 10450, *Security Requirements for Government Employment*
- EO 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984
- EO 12656, *Assignment of Emergency Preparedness Responsibilities (COOP Plans)*, November 18, 1988, as amended by EO 13074
- EO 12958, *Classified National Security Information*
- EO 12968, *Access to Classified Information*, August 1995
- EO 13011, *Federal Information Technology*, July 16, 1996
- Office of Management and Budget (OMB) Bulletin 90-08, *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems That Contain Sensitive Information*, July 9, 1990
- OMB Circular No. A-123, *Management Accountability and Control*, June 1995
- OMB Circular No. A-127, *Financial Management Systems*
- OMB Circular No. A-130, *Management of Federal Resources,* Appendix III, Security of Federal Automated Information Resources, February 8, 1996 (revision of edition issued December 24, 1985)
- Presidential Decision Directive 39 (PDD-39), *Policy on Counter-Terrorism*
- PDD-62, *Combating Terrorism*
- PDD-63, *Critical Infrastructure Protection*, May 22, 1998
- PDD-67, *Continuity of Government (COG) and Continuity of Operations (COOP) Plans*

United States Department of Commerce, National Institute of Standards and Technology (NIST)

- NIST, *Federal Information Processing Standards* (FIPS)
- NIST Special Publication (SP) 800-2, *Public Key Cryptography*
- NIST SP 800-3, *Establishing a Computer Security Incident Response Capability*
- NIST SP 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*
- NIST SP 800-5, *A Guide to Selection of Anti-Virus Tools and Techniques*
- NIST SP 800-6, *Automated Tools for Testing Computer System Vulnerability*
- NIST SP 800-7, *Security in Open Systems*
- NIST SP 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*
- NIST SP 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, March 16, 1995
- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 1996
- NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, 1998

United States Department of Defense (DOD)

- *DOD Trusted Computer System Evaluation Criteria* (Orange Book)
- *Guidance for Applying the DOD Trusted Computer System Evaluation Criteria in Specific Environment* (CSC-STD-003-85) (Yellow Book)
- *DOD Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements* (Yellow Book)
- *DOD PC Security Considerations* (Light Blue Book)
- *DOD Password Management Guideline* (Green Book)
- *DOD Guide to Understanding Audit in Trusted Systems* (Tan Book)
- *DOD Guide to Understanding Discretionary Access Control in Trusted Systems* (Orange Book)
- *DOD Guide to Understanding Configuration Management in Trusted Systems* (Orange Book)
- *DOD Glossary of Computer Security Terms* (Aqua Book)
- DOD Directive 5200.28, *Security Regulations for Automated Data Processing*
- National Security Telecommunications and Information Systems Security Committee (NSTISSC) *Policy 200 on Controlled Access Protection*, July 15, 1987
- NSTISSC *Policy 300 on Control of Compromising Emanations*, November 29, 1993
- NSTISSC *Directive 500 on Telecommunications and Automated Information Systems Security (TAISS) Education, Training, and Awareness*, February 25, 1993
- NSTISSC *Directive 600 on Communications Security (COMSEC) Monitoring*, April 10, 1990

United States General Accounting Office (GAO)

- *GAO Executive Guide: Information Security Management, Learning From Leading Organizations*, May 1998
- *GAO Information Security, Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, September 1998
- *GAO Year 2000 Computing Crisis, Potential for Widespread Disruption Calls for Strong Leadership and Partnerships*, April 1998
- *GAO Federal Information System Controls Audit Manual (FISCAM)*, January 1999

Other Authorities and Guidance

- Critical Infrastructure Assurance Office (CIAO), *Vulnerability Assessment Framework Version 1.1*, prepared under contract for CIAO by KPMG Peat Marwick LLP, October 1998
- Director of Central Intelligence Directive (DCID) 1/14, *Personnel Security Standards*, July 2, 1998
- DCID 1/16, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks*, 1988
- DCID 1/21, *Physical Security Standards for Sensitive Compartmented Information (SCI) Facilities*, July 29, 1994
- President's Commission on Critical Infrastructure Protection (PCCIP) Report, *Critical Foundations: Protecting America's Infrastructures*, October 1997
- United States Department of Justice, *Vulnerability Assessment of Federal Facilities*, June 1995

Appendix C. NSA INFOSEC Assessment Methodology

With the increased complexity and reliance on information systems and the proliferation of threats to information confidentiality, integrity, and availability, information systems security (INFOSEC) is becoming more important to missions critical to national security. The National Security Agency (NSA) has developed an INFOSEC Assessment Methodology (IAM) to provide assistance to Presidential Decision Directive 63 (PDD-63) departments and agencies in assessing their INFOSEC postures. The IAM is a Critical Infrastructure Assurance Office- (CIAO-) endorsed methodology to be used as the baseline standard for cyber vulnerability analysis. Through implementation of the IAM, the depth and scope of baseline vulnerability assessment efforts can be standardized across PDD-63 agencies and departments.

The IAM provides a high-level, comprehensive review of the INFOSEC posture of an organization's operational system(s). The IAM will assist in identifying critical missions, information systems critical to those missions, and potential systems security vulnerabilities. In addition, recommendations are provided to eliminate or mitigate the identified vulnerabilities to enhance the INFOSEC posture.

The baseline IAM is nonintrusive and does not include hands-on testing. This reduces the time required to coordinate and perform the assessment. The assessment will identify many areas for the improvement of an organization's INFOSEC posture, as well as define areas where further analysis (e.g., testing) is needed. The results of the INFOSEC assessment analysis will identify many problems and solutions and will focus future analytical efforts. The goal is to allow the recipients to make more informed risk management decisions.

The IAM is a three-phase approach. The first phase is preassessment. Preassessment is usually performed at the customer's site and lasts from one to two days. During this time, the assessors assist the customer in identifying and defining the missions critical to the organization and the information required to perform those missions. Next, this information is analyzed to evaluate the various impacts that information compromise, loss of integrity, loss of availability, and other relevant occurrences have on each critical mission. Then the information systems that process, transmit, and store this information are identified. The scope of the assessment is then determined by the number and location of the critical system(s). The final part of the pre-assessment phase is the request for systems documentation. The assessors will request various security and user documents for review to become more familiar with systems and applications before the onsite assessment phase.

Once the preassessment phase is concluded, an assessment plan is drafted. This plan is used to record the information from the preassessment phase, coordinate future phases, and keep track of the assessment. Information in the plan is added to and updated throughout the assessment.

The onsite assessment (second phase) usually lasts from one to two weeks. It begins with an in-brief meeting. At this meeting, the assessment plan is reviewed to make sure the scope and efforts of the assessment are agreed upon. The majority of the onsite assessment phase is spent gathering information about the security posture of the system(s). This information is gathered primarily through interviews with various individuals, who may include security administrators, system administrators, upper management, and users of the various applications. Additional

documentation is also reviewed onsite as needed. Because no hands-on testing is performed, the assessment team members will request system demonstrations where they can observe a user or administrator performing various security-related functions.

The onsite assessment phase concludes with an out-brief of the initial findings and recommendations. This allows the customer to start making improvements to the INFOSEC posture. It also gives the customer an opportunity to ask questions and provide feedback to the assessment team. The assessment plan is updated to reflect the onsite phase events.

The third phase is final analysis and report generation. The assessment team performs any additional research, documentation review, and/or information gathering and generates a report. The report identifies potential vulnerabilities and provides various recommendations to raise the overall INFOSEC posture. The report is given only to the requesting individual and all information and analysis is treated as proprietary.

The IAM is a detailed and systematic way of examining cyber vulnerabilities, developed by experienced NSA INFOSEC assessors. NSA has attempted to use the IAM to assist both INFOSEC assessment suppliers and consumers requiring assessments. This market created by the PDD-63 requirement for vulnerability assessments of automated information systems that support the U.S. infrastructure is very large. In addition to assisting the Governmental and private sectors, an important result of supplying baseline standards for INFOSEC assessments will be the fostering of a concomitant improvement in PDD-63 organizations' security posture.

NSA does not have the resources to perform enough INFOSEC assessments to meet the demand. In order to increase the suppliers of IAM assessments, therefore, NSA has developed a two-day IAM training course. This course has two target audiences.

- *PDD-63 agencies' and departments' INFOSEC analysts.* These individuals will be trained in the IAM so they can use their INFOSEC analysis skills, along with the IAM training, to provide standardized IAM service for their own organization. Because the IAM is a baseline methodology, the final results of the assessment service are highly dependent on the INFOSEC and analytic skills of the assessors. For this reason, it is suggested that individuals have either the proper experience or take additional INFOSEC training before taking the IAM course.

  To further assist the agencies and departments, NSA can provide an assessor to be part of a team for IAM students' initial assessment. This allows a group of IAM-trained individuals to perform an assessment with the assistance of an experienced assessor. Once the first assessment is completed, the team members will have gained valuable experience and can carry out additional assessments for their organization.

- *INFOSEC assessment service providers.* Currently, companies and Government organizations looking for outside help assessing the security posture of their information systems can choose from dozens of commercial firms that advertise INFOSEC assessment capabilities. Although these contractors all provide INFOSEC assessment services, their processes, terminology, scope, and costs vary widely. For the benefit of prospective assessment customers, many of whom are agencies and departments trying to comply with PDD-63, NSA has developed an INFOSEC Assessment Training/Rating Program.

The Assessment Training/Rating Program is designed to offer commercial and Government organizations standardized guidance and training for defining, conducting, and improving their INFOSEC assessment process. NSA has proposed that this program be sponsored by the National Information Assurance Partnership (NIAP); in the meantime, NSA is implementing an interim program to perform these functions.

The program concept assumes that customers are looking for providers who can perform a competent INFOSEC assessment. The program offers providers guidance and training to improve their competency and publicizes provider competency ratings to help customers make their decision.

The first step for INFOSEC assessment service providers interested in the Assessment Training/Rating Program is to be formally trained in the IAM. NSA periodically schedules IAM classes and makes them available to service providers who meet the qualifications. To receive an NSA Certificate of Completion, students must demonstrate an understanding of the IAM through participation in group projects and achieve a passing score on the written IAM test. A list of these students will eventually be made public for prospective INFOSEC assessment customers.

If an organization qualifies, it can be appraised against the INFOSEC Assessment Capability Maturity Model (IA-CMM) and receive a rating profile that reflects the maturity of its processes that support the performance of INFOSEC assessments. NSA used the System Security Engineering Capability Maturity Model as a baseline to develop the IA-CMM. Each participating INFOSEC assessment service provider receives a rating for each of nine process areas. The ratings range from 0 (does not perform the process) to 5 (the process is institutionalized, is measured for quality, and is constantly being improved). Each participating provider will have representatives trained in the IAM so that the processes will reflect the standardized assessment methodology implementation.

Prospective INFOSEC assessment customers can review the IAM and IA-CMM documents and decide if an INFOSEC assessment will meet their requirements. They can then check the list of INFOSEC assessment service providers and the latest IA-CMM rating profiles for INFOSEC assessment service provider organizations. Customers then contact one or more of the providers directly to negotiate and contract for the service.

On the following pages are guidelines for letters requesting an INFOSEC assessment and IAM training.

INFOSEC ASSESSMENT REQUEST LETTER GUIDELINE

Below is a guideline to assist in preparing a letter of request for an INFOSEC assessment. Feel free to include any other information that you consider relevant. If you have questions, please contact the Chief, INFOSEC Assessment Division, who can be reached at (410) 854-7821.

<date>

To: DIRNSA
National Security Agency
Attn: DDI, X64, (410) 854-7821
9800 Savage Road (SAB 3)
Ft. Meade, MD 20755

The <*company/organization name and location*> requests the National Security Agency perform an INFOSEC assessment of our <*system(s) name and location (if different than above*)>.

(required information)

<Paragraph(s) explaining what the company/organization does, including major missions and customers.>

<Paragraph(s) explaining what the system is used for, to include the sensitivity of the data stored, processed, and transmitted by the system (unclassified, proprietary, classification, etc.)>

(optional information)

<Any specific INFOSEC concerns related to the system.>

<Approximate time frame or time constraints for the onsite visit or completion of the final report.>

(required information)

Our point of contact for the assessment process is *<name, title, phone number>*.

<Name of requester>
<Title of requester>

INFOSEC ASSESSMENT METHODOLOGY CLASS
REQUEST LETTER GUIDELINE

The following is a guideline to assist in preparing a letter of request for the two-day INFOSEC Assessment Methodology (IAM) training class. Feel free to include any other information that you consider relevant. If you have questions, please contact the Chief, Critical Infrastructure Protection Support Division, at (410) 854-7827.

<date>

To: DIRNSA
National Security Agency
Attn: DDI, X61, (410) 854-7827
9800 Savage Road (SAB 3)
Ft. Meade, MD 20755

The <*company/organization name and location*> requests training in the National Security Agency INFOSEC Assessment Methodology.

<Paragraph(s) explaining what the company/organization does, including major missions and customers.>

<Paragraph(s) explaining the sensitivity of the data stored, processed, and transmitted by the organization (unclassified, proprietary, classification, etc.), including how it relates to the national critical infrastructure.>

<Approximate time frame in which the training is required.>

<Number of students to be trained (minimum of 20 and maximum of 36 students).>

<Preferred location of the IAM class (e.g., NSA facility, onsite, etc.).>

<Point of contact (name, title, phone number).>

<Name of requester>
<Title of requester>

(this page purposely left blank)

Appendix D. Cryptographic Technology Deployment Issues

Key Management

Public Key Certification

To deploy asymmetric cryptographic technology (also called public key technology), users must make their public keys widely available. This is not a simple process, and there are potential pitfalls. When you access the public key of another user, you want to be sure that the public key does indeed belong to that user and not to someone masquerading as him or her. If you are acquainted with the user, you can phone and have him send you his public key by email. There are many situations, however, in which you will want to send encrypted data to users you do not know and do not wish to contact before sending the data.

There must be a mechanism by which you can conveniently obtain the public keys of all users with whom you wish to exchange cryptographic data and be assured that the public keys you obtain are authentic. Certification authorities (CAs) exist to provide the latter service and may also provide the former. A CA issues a certificate that binds a user's identity to a public key. The certificate attests that the CA has verified that the public key contained in the certificate was issued to the user listed. The CA publishes the procedures by which the user's identity has been authenticated so that users will have confidence in the certificates that it issues. The CA need not have access to the user's private key in order to provide the authentication service; the certificate merely states that the listed user has presented this public key to the CA, and the CA has verified that the user is who he says he is.

After the certificate is issued, it should be published either by the user or the CA in a publicly accessible database. The Lightweight Directory Access Protocol (LDAP) has become the *defacto* standard for accessing public key certificates from a certificate repository. LDAP is a scaled-down version of the Directory Access Protocol, which was developed by the International Telecommunications Union.

The key management issue is complicated by the fact that there are many CAs issuing certificates. A user may trust the certificates issued by his local CA, but how does he or she know to trust the certificates issued by other CAs? Even if the authentication procedures of these CAs are published, users cannot be reasonably expected to review them, nor can they know whether the authentication is being performed as stated in those procedures. For users to be able to trust the certificates issued by non-local CAs, there has to be a method by which the CAs can scrutinize and approve one another. For example, CA1 and CA2 could agree to review each other's procedures and audit implementation to ensure that the individuals responsible for authentication are doing it correctly. This pairwise approval process will not work, however, if there are many CAs involved. A better solution would be to arrange the CAs in a hierarchy in which those at one level are responsible for reviewing and approving the procedures used by those at the level below. The chain of CAs that attests to the authenticity of the user certificate would be bound and distributed with the certificate. At the top of the hierarchy would be a CA in which everyone has confidence, called the "Root CA."

This solution has not yet been widely implemented, although it is in place in a few user communities. The obstacles are more behavioral than technical. Despite minor interoperability problems among products, vendors now market software that can establish such a hierarchical trust relationship among CAs, and current applications are able to recognize that such a relationship exists. CAs, however, must join forces to develop policies and standards that will allow them to recognize and accept each others' certification procedures and certificates.

Encryption Standards

The most popular symmetric-key encryption algorithm currently is the Data Encryption Standard (DES). DES is a block cipher; it encrypts data in 64-bit blocks. The algorithm was developed by IBM, who gave up royalty rights and allowed the algorithm to be placed in the public domain. The National Institute of Standards and Technology (NIST) adopted DES as a Federal standard in 1976, and the American National Standards Institute (ANSI) adopted DES as a private-sector standard in 1981. A variant of DES, Triple DES, has also been widely implemented. Triple DES operates on a block of data three times with two keys: with the first key, then with the second key, and finally with the first key again. Although these standards have served their purpose well, a search is underway for a symmetric encryption algorithm for the 21st century that will anticipate the vastly improved computer technology that will be available to break encryption codes. NIST has launched a worldwide search for an algorithm to form the basis of an Advanced Encryption Standard and is currently evaluating proposals. A selection will be made within the next few years.

The most widely used asymmetric-key algorithm is RSA. It is one of the few asymmetric-key algorithms that can be used to provide both a digital signature and encryption service. One barrier to even wider usage of RSA has been that RSA has a patent on the algorithm, which means that the patent holder can charge for each generated public/private key pair (but the patent expires in 2000). Partly because of the patent issue, NIST adopted the Digital Signature Algorithm (DSA), developed by the National Security Agency (NSA) as the Digital Signature Standard in 1994. The DSA, however, provides only a digital signature service, not an encryption service. The algorithm most frequently selected to perform encryption is the Diffie-Hellman algorithm, developed by Whitfield Diffie and Martin Hellman, who invented asymmetric-key cryptography in the 1970s. Recently, NIST proposed a revision to the Digital Signature Standard, which would allow either RSA or DSA to provide the digital signature service and would allow the RSA algorithm to be used to provide an encryption service as long as different public/private key pairs are used for signing and encrypting.

The two principal algorithms used in cryptographic applications for compressing data are the Secure Hash Algorithm (SHA) and Message Digest 5 (MD5). The SHA was designed by NIST and NSA and issued as the Secure Hash Standard by NIST. The Secure Hash Standard states that the SHA is to be used whenever a message digest algorithm is required for Federal applications. The SHA produces a 160-bit hash of the message contents. MD5, the other widely used algorithm, was designed by Ron Rivest of RSA and produces a 128-bit hash of the message contents. Many cryptographic applications can generate and process both algorithms.

A family of Public Key Cryptography Standards, developed by RSA in cooperation with a group of vendors, exists to provide an industry-standard interface for asymmetric-key cryptography.

The standards specify the syntax for the header of an encrypted and signed message, the syntax for public key certificates, the syntax for a user request to a CA to issue a certificate, and a syntax for private key information. Although these standards have not been officially endorsed by any standards body, they have become *de facto* standards that have been widely implemented.

Key Recovery

It is essential that users protect their private keys from disclosure. Commercial implementations of cryptographic technology provide such mechanisms as passwords for this purpose. Users, however, can forget their passwords. They can also die or leave an organization without revealing their passwords, leaving behind information essential to the operation of a business in encrypted form. Any cryptographic application must include a means of providing emergency access to encrypted data, called key recovery. Each organization using cryptography must determine who is authorized to obtain emergency access to a user's encrypted data and under what circumstances, and communicate this policy to all members of the organization.

Various commercial key recovery applications exist. Some permit an authorized third party to gain access to all information that has been encrypted with a user's private key with a single request. In other applications, the symmetric message encryption key is encrypted with the public key of an authorized key recovery center. A separate request must be made to the key recovery center for each message for which decryption is desired.

The Future

The technology that provides the cryptographic services listed above is still is in the early stages of development. Some interoperability issues among the products of different vendors remain unresolved. Most operational implementations rely on the product of a single vendor to provide a specific service to a closed community. There are also nontechnical issues that have to be addressed. Users must agree on policies for using asymmetric-key technology so that, for example, a user can trust a public-key certificate issued by a nonlocal CA. A driving force for resolving these issues is likely to be an application, such as secure email, that is desired by many users and that requires widespread deployment of a supporting public key infrastructure. Federal agencies are currently working with each other and with vendors to remove the barriers to making a secure email service available to all Federal Government users.

For Additional Information

Access With Trust, issued jointly by the Federal Infrastructure Steering Committee, the Government Information Technology Services Board, and the Office of Management and Budget, is available at the Web site http://gits-sec.treas.gov/gits-sec-home.htm .

Appendix E. Low-Cost/No-Cost Computer Security Measures

Below is a list of no-cost/low-cost measures that can be implemented to increase the overall level of security on computer systems.

Password Dos and Don'ts

1. *Do not* use your login name as your password.
2. *Do not* use your first, middle, or last name as your password.
3. *Do not* use the names of your family members as your password.
4. *Do not* use license plate numbers, phone numbers, social security numbers, makes of cars, or street names as your password.
5. *Do not* use a single number or letter in a series (111111 or aaaaaa) as your password.
6. *Do not* use consecutive numbers or letters (123456 or abcdef) as your password.
7. *Do not* allow "keyboard progression" passwords (i.e., qwertyui or lkjhgfds)
8. *Do not* use numbers at the beginning or end of passwords.
9. *Do not* create your password using a word from an English or foreign-language dictionary.
10. *Do not* use a password shorter than six characters. A minimum of eight characters would be more secure.
11. *Do not* share passwords with anyone.
12. *Do not* allow group accounts with a common password.
13. *Do* use a password with mixed-case alphabetic characters, numbers, and symbols.
14. *Do* use an easy-to-remember password, but *do not* write it down. As a mnemonic device, use the initial letters in a phrase. (For example: IL2PGitS!—I love to play golf in the summer!)
15. *Do* change passwords every 90 to 120 days, but *do not* reuse old passwords.
16. *Never* use passwords in the clear over modems.
17. Have the system administrator run a "password cracker" program at least every three months, preferably more often, and require users to immediately change any easily cracked passwords.

System Monitoring

1. Ensure system audit features are active on the system.

2. Protect the audit trail so that no normal user can view or modify the audit log.

3. Do not allow multiple logons. If an employee is allowed to logon to his/her workstation and then walk around the corner and logon to another workstation with the same logon ID and password, the audit trail can no longer track the user as precisely as security needs require. If both terminals are active with the same logon, the system can never be sure if the authorized user is on the system or if someone else is using his/her account.

4. Review audit trails for security-related incidents as well as for "health" of the system on a regular basis (daily if possible).

5. If the option exists, display, with a pause, the last unsuccessful logon attempt on the workstation screen.

6. Do not allow sniffer boxes to run unattended or unsecured.

7. Provide all users of the system with "security alert" announcements.

General Security Administration and Awareness

1. Assign a system security officer to each computer area and set of workstations.

2. Provide adequate training for all system administrators, system security officers, and LAN maintenance personnel.

3. Implement a security awareness program. The program should include orientation for new users as well as annual training for veteran users.

4. Turn on security features provided by the system vendor.

5. Develop a prioritized list for security enhancements/upgrades.

6. Ensure that all users know the correct procedure for reporting security problems. This can be part of the annual security training program.

7. Ensure that all users know what to do with their computers and media when responding to a fire alarm or other emergencies requiring evacuation.

8. Establish and regularly review policies and procedures for equipment maintenance and physical security.

9. Ensure that all users understand the policies and procedures for moving data from one system to another, particularly if the systems operate at different levels of sensitivity/classification.

10. Ensure all users know the current policy on reuse of computer components and magnetic media.

11. Employ warning banners that cover security and other issues of concern (For example: "Contains proprietary information . . . disclosure to unauthorized personnel punishable by law" or "Use of system constitutes permission to monitor. . .") *Note*: have the language in warning banners reviewed by the agency general counsel or legal department.

12. Standardize account request forms and procedures to simplify audit reviews.

13. Standardize help desk verification and account reset procedures.

14. Establish end-of-day procedures for closing down individual work areas.

Access Control

1. Direct users to lock their computer screens every time they leave their computers. Never give someone (who may not have file access privileges) the opportunity to use an account other than his or her own; it negates the use of audit trails for tracking. Use a password-protected screensaver initiated by the user or activated after a specified period of inactivity.

2. If logon sessions are inactive for more than 10 minutes, lock the screen or account. The owner will have to enter his/her password to unlock the screen/account.

3. Secure all removable storage media at the end of the day.

4. Tightly control the use of unclassified computers in classified areas. Unclassified computers should be turned off when not in use.

5. Delete all guest accounts. When a guest needs the use of a computer, establish a new account and password with proper access controls. When the guest leaves or no longer needs the use of the computer, delete the account.

6. When a user changes jobs, retires, quits, or is terminated, disable the account for a set period of time (e.g., three months). This allows coworkers to access it for documents or email related to ongoing projects. After a set period, purge the account from the system.

7. Limit users' access to floppy disk drives and CD-ROM drives.

8. Keep access privileges (read, write, exec, etc.) current and limited to the minimum required to do the job.

9. Verify that physical access security devices for computer facilities are current. This includes keeping tables for badge swipes up to date and changing door combinations when required.

10. Control access to the computer room. Escort outside maintenance personnel and other visitors.

11. Have someone other than a manager or administrator verify, on a regular or random basis, that firewall or router IP access control lists are accurate and current.

12. When using office-issued laptops, be sure to handle and maintain them properly.

13. Turn computer screens away from open windows.

Configuration Management

1. Ensure that system documentation such as security plans, concepts of operations, and configuration management plans contain an accurate description of all interfaces with other systems, sites, or agencies.

2. Eliminate all connections to critical systems that are unrelated to their primary functions.

3. Do not allow users to download files from the Internet without a screening process in place.

4. Know what hardware and software is on the system/network. Establish a Configuration Control Board or process for tracking hardware/software in place and for installing and testing patches and upgrades on a timely basis.

5. Limit authority for adding new software or upgrading current software to system administrators.

6. Use modems only when necessary, preferably in a modem pool configured to be outside the firewall (see Chapter III, Access Control). Turn off modems when not in use, and disconnect them when practical and/or possible.

7. Do not make the Web server part of the network (local or wide area). A Web server on the network could provide an additional path to protected information.

Protection of Information

1. Know the value of the information being processed and why it should be protected. Add this information to security awareness training for the new user as well as the annual security awareness training program.

2. Eliminate storage of critical information at local workstations, to reduce both the chance of unauthorized access and the chance of accidental loss or destruction (for example, from a hard drive failure).

3. Make backups of data files and system files.

4. Store backup files securely offsite, in a location from which they can be retrieved within the time required for resuming system operation.

5. Use antivirus software that contains a virus scanner. Scan *all* files entering the system, not just files from across the Internet.

6. Always use the latest version of the authorized antivirus software.

7. If users work outside the office and bring their output to work on disks and diskettes, require scanning of all such removable storage media before files are copied to an office workstation or laptop.

8. Label all information on removable storage media with the level of sensitivity/classification.

9. Dispose of damaged removable storage media in an approved container.

10. Dispose of all printouts in an approved container.

Disaster Recovery

1. Make sure there is a disaster recovery plan in place.

2. Test the disaster recovery plan once a year. If it is not practical to test the plan by shutting down the entire system, test it module by module, while the rest of the system remains in operation.