Order Code RL32357

CRS Report for Congress

Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives

April 16, 2004

John Moteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Prepared for Members and Committees of Congress

Computer Security: A Summary of Selected Federal Law, Executive Orders, and Presidential Directives

Summary

This report provides a short summary of selected federal laws, executive orders, and presidential directives, currently in force, that govern computer security. The report focuses on the major roles and responsibilities assigned various federal agencies in the area of computer security. This report will not be updated.

One major area of federal activity in computer security deals with securing federal computer systems. The roles and responsibilities for securing federal computer systems are split between national security systems and all other federal systems. The Federal Information Security Management Act of 2002 authorizes the Director of the Office and Management and Budget to oversee the development of, and compliance with, security standards and guidelines, developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce. These authorities, however, do not apply to computer systems considered to be national security systems. The roles and responsibilities for securing national security systems are established by National Security Directive 42 (NSD-42). NSD-42 establishes what is now called the Committee on National Security Systems, which it authorizes to develop, and require compliance with, standards and guidelines for national security systems.

In general, the federal government does not regulate the security of non-government computer systems. However, the federal government does require certain information held on non-government systems to be protected against unauthorized access and disclosure, primarily out of privacy considerations. To date, this has been limited to financial information (Gramm-Leach-Bliley Act) and medical information (Health Insurance Portability and Accountability Act of 1996). A number of regulatory agencies have authority for developing and enforcing standards for financial information. The Secretary of Health and Human Services has authority to develop and enforce standards for medical information. The Sarbanes-Oxley Act of 2002 requires certain companies to certify the accuracy of their internal financial controls. The Security Exchange Commission has authority to develop standards and enforce these regulations.

Although it currently has a limited role in securing the nation's overall information infrastructure, the federal government does, through the Department of Homeland Security, work with and encourage the private sector, state and local government, academia, and the general public to protect the nation's information infrastructure. This role is authorized in a generic sense for all critical infrastructure by the Homeland Security Act of 2002. It is also reinforced more specifically in Homeland Security Presidential Directive No. 7 and the National Strategy for Securing Cyberspace. To date, these activities are voluntary for non-federal entities.

Other roles established for the federal government include: investigation and prosecution of federal computer crimes; assisting state and local law enforcement entities in their investigation and prosecutions; and, developing the nation's expertise in information security.

Contents

Computer Security: A Summary of Selected Federal Law, Executive Orders, and Presidential Directives

Introduction

This report provides a short summary of selected federal laws, executive orders, and presidential directives, currently in force, that govern computer security. The report focuses its discussion of the roles and responsibilities for computer security that have been assigned different federal departments and agencies, some of which were assigned 20 or more years ago.

This report is primarily concerned with the security of computer systems and the electronic information contained on, or transmitted by, those systems from unauthorized access, use, disclosure, disruption, modification or destruction, in the context of information services. The report does not discuss broader issues associated with information assurance which includes such concerns as the marking and handling of information in both electronic and physical formats, the assignment of certain status to certain types of information, and determining who should and should not have authorized access to it. The report also touches on telecommunications to a limited extent. Even though the technologies associated with computers and telecommunications have become inextricable, there remains a distinction between the use of that technology for information services (i.e. the Internet) and its use, in some cases of the very same hardware, for telecommunication services.

The major federal role and responsibility in computer security relate primarily to securing federally owned, leased, or operated systems (or those systems operated for the federal government under contract or by third parties). In general, the federal government does not regulate the security of non-government computer systems (other than those used by contractors for the federal government). However, the federal government does require certain information held on non-government systems to be protected against unauthorized access and disclosure. In addition, as part of its effort to enhance the security of the nation's critical infrastructure, the federal government is working with and encouraging the private sector to improve security of the nation's information infrastructure more generally.

Another role the federal government plays in computer systems security is to investigate and prosecute federal computer crimes. The federal government also offers assistance to state and local law enforcement entities in their investigation and prosecution of computer activities made illegal at the state level. Finally, the federal government has programs in research and development and in the development of the nation's expertise in computer security.

Securing Federal Computer Systems

Non-National Security Systems. Building upon the Computer Security Act of 1987 (P.L. 100-35), the Paperwork Reduction Act of 1995 (P.L. 104-13), and the Information Technology Management Reform Act of 1996 (i.e. Clinger-Cohen Act, P.L. 104-106, Division E), the **Federal Information Security Act of 2002** (P.L. 107-347, Title III) provides the basic statutory requirements for securing federal computer systems. The Federal Information Security Act (**FISMA**) requires each agency to inventory its major computer systems, to identify and provide appropriate security protections, and to develop, document, and implement an agency-wide information security program.

FISMA authorizes the National Institute of Standards and Technology (NIST) to develop security standards and guidelines for systems used by the federal government. It authorizes the Secretary of Commerce to choose which of these standards and guidelines to promulgate. FISMA authorizes the Director of the Office of Management and Budget (OMB) to oversee the development and implementation of (including ensuring compliance with) these security policies, principles, standards and guidelines.

To help fulfill his responsibilities, FISMA authorizes the Director of OMB to: require agencies to follow the standards and guidelines developed by NIST and prescribed by the Secretary of Commerce; review agency security programs annually and approve or disapprove them; and, take actions authorized by the Clinger-Cohen Act (including budgetary actions) to ensure compliance.

FISMA also requires agencies to conduct, annually, an independent evaluation of their security programs which includes an assessment of the effectiveness of the program, plans, and practices and compliance with FISMA requirements. The result of those evaluations are forwarded to the Director of OMB, who is to summarize the results each year in a report to Congress.

FISMA also directs the Director of OMB to "ensure the operation" of a federal information security incident center. Among the missions of this center are: providing timely technical assistance to federal agencies in detecting and handling computer incidents; and, compiling and analyzing incident data. Such a center existed prior to FISMA. The Federal Computer Incident Response Capability (FedCIRC) evolved out of a pilot project first begun at NIST in 1996. FedCIRC was transferred to the General Services Administration, before being transferred again to the Department of Homeland Security. This capability is now located within the National Cyber Security Division in the Information Analysis and Infrastructure Protection Directorate.

The above mentioned roles and responsibilities of NIST, the Secretary of Commerce, and the Director of OMB (except for the Director's authority to take related budgetary actions and to report to Congress), do not extend to computer systems identified as national security systems.

National Security Systems. FISMA[1] defines a national security system, in statute, as:

> Any computer system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
>
> (i) the function of which—
>
> (I) involves intelligence activities;
> (II) involves cryptologic activities related to national security;
> (III) involves command and control of military forces;
> (IV) involves equipment that is an integral part of a weapon or weapons system;
> (V) ...is critical to the direct fulfillment of military or intelligence missions; or
>
> (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

The definition explicitly excludes systems that are used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

The roles and responsibilities for securing national security systems are outlined in **National Security Directive 42 (NSD-42)**, signed July 5, 1990 by President George H. W. Bush.

NSD-42 establishes the National Security Telecommunications and Information Systems Security Committee, now called the Committee on National Security Systems (CNSS).[2] CNSS is an interagency committee, chaired by the Department of Defense. Among other assignments, NSD-42 directs the CNSS to: provide system security guidance for national security systems to executive departments and agencies; and, submit annually to the Executive Agent (see below) an evaluation of the security status of national security systems. NSD-42 also directs the Committee to interact, as necessary, with the National Communications System Committee of Principals (see below).

NSD-42 assigns membership to the Committee to voting representatives of the Secretaries, Directors, and Administrators of the following departments and agencies: State, Treasury, Defense, Commerce, Transportation, Energy, Office of Management

---

[1] P.L. 107-347,§ 301(b)(1).

[2] The name was changed by Executive Order (E.O.) 13231, signed October 16, 2001. E.O. 13286, signed February 28, 2003, and which amended E.O. 13231, kept the name change.

and Budget, Central Intelligence,[3] Federal Bureau of Investigations, Federal Emergency Management Agency (FEMA), General Services Administration, National Security Agency, Defense Intelligence Agency. Also included are: the Attorney General, the Assistant to the President for National Security Affairs, Chairman of the Joint Chief of Staff, the Chiefs of Staff of the Army and the Air Force, the Chief of Naval Operations, the Commandant of the Marine Corps, and the Manager of the National Communications System (NCS). FEMA and NCS are now parts of the Department of Homeland Security.

NSD-42 names the Secretary of Defense as the Executive Agent of the Government for National Security Telecommunications and Information Systems Security. NSD-42 directs the Executive Agent to implement policies and procedures that: ensure the development of plans and programs necessary to secure national security systems; procure for, and provide to, executive departments and agencies technical security materials, and other technical assistance; conduct, approve, or endorse research and development of security techniques and equipment; and to operate or coordinate the activities of federal technical centers related to national security systems. NSD-42 also assigns to the Executive Agent the responsibility for reviewing and assessing the National Manager's (see below) recommendations on national security systems programs and budgets for executive departments and agencies. The Executive Agent may make appropriate budgetary and programmatic recommendations to agency heads as well as to the National Security Council and to the Office of Management and Budget. In addition, NSD-42 instructs the Executive Agent to report the security status of national security systems to the President through the National Security Council.

NSD-42 also designates the Director of the National Security Agency as the National Manager for National Security Telecommunications and Information Systems Security. Among the authorities granted the National Manager are: examine U.S. Government national security systems and evaluate their vulnerability to foreign interception and exploitation; conduct, approve, or endorse research and development of security techniques and equipment; review and approve all security related standards, techniques, systems, and equipment for national security systems; assess the overall security posture of and disseminate information on threats to and vulnerabilities of national security systems; operate a central technical center to evaluate and certify national security systems; prescribe minimum standards, methods, and procedures for protecting national security systems; annually review and assess the national security systems programs and budgets of department and agencies, individually and in the aggregate, and recommend alternatives to the Executive Agent; and, enter into agreements for the procurement of technical security materials and equipment and their provision to executive departments and agencies, and when appropriate, to government contractors and foreign governments.

---

[3] The Director of Central Intelligence also cites (Director of Central Intelligence Directive 6/3-Policy) his authority to protect intelligence sources and methods granted under the National Security Act of 1947, Executive Orders 12333 and 12958, and NSD-42, to develop, and require compliance with, standards and guidelines to protect intelligence information on computer systems.

Summary. To summarize, the Director of OMB is authorized to oversee the development of, and ensure compliance with, policies, principles, standards and guidelines governing the security of all federal computer systems, except for national security computer systems. The Committee on National Security Systems has that authority for national security systems (which include both information and telecommunication systems). The Director of Central Intelligence cites similar authority for computer systems that contain intelligence information. NIST has the responsibility for developing security standards and guidelines for all federal computer systems, except national security systems. The National Security Agency has that authority for national security systems.

National Strategy. Although carrying less authority than law, executive order, or presidential directive, the ***National Strategy to Secure Cyberspace***, released in February 2003,[4] makes a number of recommendations aimed at the largest computer network operators, including the federal government, to the smallest of home users. Three recommendations direct specific federal agencies to take specific actions to improve the security of federal systems. The Strategy recommends DHS use exercises to test the security of federal systems and to report the results of those exercises to the Director of OMB. It also directs DHS to work with the General Services Administration to develop an improved patch management system, to ensure that agencies have made up-to-date security modifications to their software. The Strategy also directs OMB to coordinate the development of a research and development strategy for information technology security and to update this annually.

National Communication System. Because of the reliance of computer networks on telecommunication assets and the use of computers in telecommunication networks, and the inextricable nature of the technologies involved, it is necessary to spend a few paragraphs discussing the National Communication System. NSD-42 makes reference to the National Communication System's Committee of Principals. The National Communication System (NCS) was first established by Presidential Memorandum No. 252, signed by President Kennedy in 1963 following the Cuban Missile Crisis. The Memorandum called for establishing a NCS by linking together, and improving on an evolutionary basis, the communication facilities and components of various federal agencies. This original memorandum since has been amended and superseded over time. The Executive Order currently in force is **Executive Order 12472**, signed by President Reagan on April 3, 1984, which was amended slightly by President George W. Bush in Executive Order 13286, on February 28, 2003.

E.O. 12472 established (i.e. defined) a national communication system as those telecommunication assets owned or leased by the federal government that can meet the national security and emergency preparedness needs of the federal government, together with an administrative structure that could ensure that a national telecommunications infrastructure is developed that is responsive to national security and emergency preparedness needs. The administrative structure includes a National

---

[4] The Strategy was released by the President's Critical Infrastructure Protection Board. The Board was established by Executive Order 13231 (October 18, 2001). The Board was dissolved by Executive Order 13286 (February 28, 2003).

Communication System Committee of Principals, an Executive Agent, and a Manager.

The National Communication System Committee of Principals consists of those agencies, designated by the President, that own or lease telecommunication assets identified as part of the National Communication System, or which bear policy, regulatory, or enforcement responsibilities of importance to national security and emergency preparedness telecommunications. The mission of the Committee of Principals is: to assist (including making recommendations to) the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy (OSTP), and the Director of the Office of Management and Budget (OMB) in exercising their functions and responsibilities associated with the National Communication System. Together the National Security Council, the Homeland Security Council, the Director of OSTP, and the Director of OMB, in consultation with the Executive Agent and the Committee of Principals, determine the requirements for the national communication system. The Committee of Principals also works closely with private sector service providers, which own and operate some of the assets that make up the NCS, through the National Security Telecommunication Advisory Committee.

The Committee of Principals also; acts as forum in which Members may discuss and report on ongoing and perspective national security and emergency planning plans and programs; and, ensures that the NCS is responsive, capable of satisfying priority telecommunication requirements, and survivable to the maximum extend practicable at all times, including times of crisis and emergency. Infrastructure security is specifically mentioned as one of the concerns of the NCS (Section 1(c)(3)).

The responsibilities of the Executive Agent include: designating the NCS Manager; ensuring the NCS conduct unified planning and operations; and, ensuring coordination with emergency management activities of the Department of Homeland Security. The original EO designated the Secretary of Defense as the Executive Agent. The **Homeland Security Act of 2002** transferred the NCS to the Department of Homeland Security. To reflect this change, **Executive Order 13286** made the Secretary of Homeland Security Executive Agent.

The responsibilities of the NCS Manager include preparing for consideration by the Committee of Principals: recommendations on an evolutionary telecommunications architecture to meet current and future national security and emergency preparedness needs; plans and procedures for the allocation and use, including the priorities and preferences, of federally owned or leased assets under all emergency or crisis conditions; plans and standards for reducing impediments to interoperability; tests and exercises for evaluating capabilities; budget reviews; and, implement any approved plans or programs. The Manager also chairs the Committee of Principals. As result of the transfer of the NCS to the Department of Homeland Security, the Secretary of Homeland Security, as Executive Agent, has designated the Assistant Secretary for Infrastructure Protection as the NCS Manager.

EO 12472 also established a joint industry-government National Coordinating Center (NCC) which assists in the initiation, coordination, restoration, and

reconstruction of national security and emergency preparedness telecommunication services or facilities under all conditions.

Protecting Information on Private Systems

There are currently no general federal requirements for private entities other than federal contractors operating systems for the federal government to secure their computer systems. However, there are requirements for entities who hold or process certain types of personal information to ensure the confidentiality of that information. To date, this includes financial information and medical information. There is also a federal requirement that certain firms that register with the Security and Exchange Commission (SEC) must include in the financial reports an assessment of their internal financial controls. To the extent that each of these types of information is held and or processed electronically, the security of some private computer systems come under federal regulation.

Title V of the **Gramm-Leach-Bliley Act** (P.L. 106-102, 15 USC Chpt. 94, §6801 *et seq.*) requires financial institutions to protect the security and confidentiality of their customers' nonpublic personal information. The Act authorizes various federal regulatory agencies, (the Comptroller of the Currency, the Security Exchange Commission, the Federal Deposit Insurance Corporation, et al.) to coordinate the development of regulations for meeting this requirement. Each of these federal agencies is authorized to enforce the regulations for those institutions in their jurisdiction. The regulations (16 CFR Part 314) require financial institutions to develop, implement, and maintain a comprehensive information security program that contains appropriate administrative, technical, and physical safeguards. Such a program should include the designation of an employee to coordinate the program, risk assessments, regular tests and monitoring of safeguards, and a process for making adjustments in light of test results and/or changes in operations or other circumstances that may impact the effectiveness of the program.

The **Health Insurance Portability and Accountability Act of 1996**, (P.L. 104-191, Title II, Subtitle F, Sec. 262, 42 USC 1320d *et seq.*) authorizes the Secretary of Health and Human Services to adopt standards that require health plans, health care providers, and health care clearinghouses to take reasonable and appropriate administrative, technical and physical safeguards to: ensure the integrity and confidentiality of individually identifiable health information held or transferred by them; to protect against any reasonably anticipated threats, unauthorized use or disclosure; and to ensure compliance with these safeguards by officers and employees. These security standards were adopted in 45 CFR Part 164, Subpart C. The Secretary assigned responsibility for enforcing these security standards to the Center for Medicare and Medicaid Services.

Besides these privacy-oriented rules, the **Sarbanes-Oxley Act of 2002** (P.L. 107-204, §404) authorizes the Security Exchange Commission to prescribe regulations requiring entities that produce annual financial reports pursuant to sections 13(a) or 15(d) of the Securities Exchange Act of 1934 to contain a report on the firm's internal financial controls. The report must state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting and assess the effectiveness of those structures

and controls. External audits must attest to and report on management's assessments. "Internal control" is defined as a process that provides assurance regarding the reliability of financial reporting. It pertains to the maintenance of records that accurately reflect the transactions and dispositions of assets and prevents or detects unauthorized acquisition, use, or disposition of assets. While there is no specific mention of computer security, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework for Enterprise Risk Management, which is mentioned in the regulation (17 CFR Part 210, 228, et al.) as the kind of evaluation process that would be acceptable, specifically includes the security of information technology (systems, software, applications) as a critical element to assess.

Working with the Private Sector

Continuing the basic policy outlined in the Clinton Administration's Presidential Decision Directive No. 63, the Bush Administration's **Homeland Security Presidential Directive No. 7 (HSPD-7)**, released December 17, 2003 states that it is U.S. policy to enhance the protection of the nation's critical infrastructure. Certain agencies were designated as lead agencies to work with their private sector counterparts. In addition to assigning the Secretary of Homeland Security the responsibility of coordinating the nation's overall efforts in critical infrastructure protection across all sectors, HSPD-7 also designates the Department of Homeland Security (DHS) as lead agency for the nation's information and telecommunications sectors. As a lead agency, DHS is to share threat information, help assess vulnerabilities, and encourage appropriate protective action and the development of contingency plans.

In addition, HSPD-7 directs the Secretary of Homeland Security to maintain an organization that serves as a focal point for securing cyberspace. That organization is to: facilitate collaboration between federal departments and agencies, state and local governments, the private sector, academia, and international organizations. Its mission includes: 24x7 analysis and warning; information sharing; vulnerability reduction; mitigation; and, aiding national recovery. The National Cyber Security Division was established within the Information Analysis and Infrastructure Protection (IA/IP) Directorate in June 2003, leveraging capabilities transferred to DHS by the Homeland Security Act of 2002, such as elements of the National Infrastructure Protection Center from the FBI and FedCIRC from the General Services Administration.

Beyond making DHS responsible for coordinating the national effort to protect critical infrastructure across all sectors, the **Homeland Security Act of 2002** also authorizes the DHS (through the Undersecretary for Information Analysis and Infrastructure Protection), as appropriate and upon request, to provide the private sector with analysis and warning of threats and vulnerabilities of computer systems. It also authorizes the Undersecretary for IA/IP, in coordination with the Undersecretary for Emergency Preparedness and Response, as appropriate and upon request, to provide the private sector with crisis management support in response to a threat or attack on critical computer systems, and technical assistance to help recover from major failures of critical computer systems. The Act also authorizes the Undersecretary for IA/IP to establish a "NET Guard" comprised of local teams of

experts to help communities respond to and recover from attacks on information and telecommunication systems.

The ***National Strategy to Secure Cyberspace***, mentioned earlier, also recommends that the Department of Homeland Security be responsible for a number of tasks associated with interacting with the state, local, and private sector. Some of these have been captured in HSPD-7. Among the recommended tasks are: establish a 24x7 synoptic view of the health of the information infrastructure; share threat and warning information; explore the use of exercises as a way to test coordination of public and private incident management, response and recovery capabilities; coordinate development of a national threat assessment; encourage a national voluntary patch clearinghouse; encourage the advanced training of cybersecurity professionals; and, encourage the development of broadly accepted certification program for those professionals.

As part of its authority to develop standards for federal computer systems, NIST is also authorized by FISMA to assist the private sector, upon request, in using and applying security standards that NIST develops.

Investigating and Prosecuting Computer Crimes

The **Counterfeit Access Device and Computer Fraud and Abuse Act of 1984** (P.L. 98-473, Title II, §2102(a), 18 USC 1030, as amended) makes certain acts associated with the unauthorized access to computers a federal crime. For example, it is a crime to knowingly gain unauthorized access to a nonpublic federal computer or a computer used by or for the federal government. It is also a crime to knowingly gain unauthorized access to a computer and obtain national security information, financial or credit information, or any information from a protected computer. A protected computer is one used by or for a financial institution, the federal government, or one used in interstate or foreign commerce and communication. It is also a federal crime to knowingly transmit a program, information, code, or command that causes damage to a protected computer. While the Attorney General has the primary authority to enforce federal laws, the Act also specifically states that the United States Secret Service has the authority, as does any other agency with such authority, to investigate the computer-related offenses covered by this section of the Act.

The **USA PATRIOT Act** (P.L. 107-56, §506(a)) amended the above statute by adding that the Federal Bureau of Investigation (FBI) has primary authority to investigate offenses where espionage or national security is involved, except for offenses affecting the duties of the United States Secret Service. Such authorities are to be exercised in accordance with an agreement signed by the Secretary of the Treasury and the Attorney General.

Section 105 of the PATRIOT Act authorizes the Director of the United States Secret Service to develop a national network of electronic crime task forces, modeled on the New York Electronic Crimes Task Force, for the purpose of electronic crimes, including potential attacks against critical infrastructure and financial payment systems. Section 816 of the PATRIOT Act also authorizes the Attorney General to establish regional computer forensic laboratories to provide forensic examinations

with respect to seized or intercepted computer evidence related to criminal activity, to provide training and education to other federal, state, and local law officials, and to assist other federal, state, and local law officials.

Some of the ground-rules for investigating computer crimes are found in the **Electronic Communications Privacy Act**. (P.L. 99-508, USC Chapters 119,121, 206). A number of these were modified in Title II of the USA Patriot Act. For example, prior to the amendments, tracking computer hackers via computer logs across jurisdictional areas required separate court orders from each jurisdiction. The USA Patriot Act allows investigators to get a single court order from any court of competent jurisdiction. Further discussion of these provisions is beyond the scope of this report.

Research and Development and Developing Information Security Expertise

The federal government has a number of programs aimed at developing computer security expertise. FISMA requires an agency's Chief Information Officer to provide training to personnel with significant security responsibilities. FISMA also requires the agency head to ensure the agency has sufficient personnel trained in information security. The Computer Security Act, which was superceded by FISMA, had authorized NIST to develop, in consultation with the Office of Personnel Management, guidelines for training agency employees in information security practices. The guidelines developed cover a range of needs from making users aware of security issues and practices to guidelines for agencies to use when developing training courses for people charged with securing computer systems. NSA has similar guidelines for training personnel in securing national security systems.

The National Security Agency, citing its authorities under NSD-42 to develop standards for securing national security system and in response to PDD-63, also has established a National Information Assurance Education and Training Program, part of which includes the National Centers of Excellence in Information Assurance Education. The Centers' program selects certain universities who have developed programs in information assurance that meet criteria established by the Committee on National Security Systems. Following the release of PDD-63, the Clinton Administration began a program called Scholarship-for-Service (SFS) which, leveraging NSA's Center of Excellence program, seeks to help schools develop information security programs that could qualify for NSA's Centers program and to support students with 2-year scholarships. Upon graduation, students receiving SFS support would be required to work 2 years in the federal sector. The National Science Foundation was tasked with running this program. The **Floyd D. Spence National Defense Authorization Act of FY2001** (P.L. 106-398, §922) authorized the Secretary of Defense to establish a similar program for the Department of Defense.

In part to help develop a cadre of experts in information security, Congress also passed the **Cyber Security Research and Development Act** (P.L. 107-305). The Act authorizes the National Science Foundation to: award basic research grants in

areas that enhance computer security; to support the establishment of multi-disciplinary Centers for Computer and Network Security Research; to award grants to institutions of higher learning to establish or improve their programs and enrollments in computer and network security; to provide graduate assistance programs in computer and network security; to establish a graduate research fellowship program; and to establish a grant program to establish university programs to train students to pursue an academic career in computer and network security. The Act also authorized NIST to support the establishment of multi-disciplinary research partnerships in computer security between universities, government, profit, and non-profit entities; and, to establish a post-doctoral research fellowship program and a senior research fellowship program.

In addition to supporting the development of national expertise in computer systems security, the federal government also conducts and supports research and development in computer systems security. As mentioned earlier in this report, NIST, DOD, and NSA are specifically authorized in FISMA and NSD-42, respectively, to conduct and support research in computer systems security. In addition, the Homeland Security Act of 2002 (Title II, Subtitle D) establishes within the Department of Justice the Office of Science and Technology. The Act authorizes this Office to conduct research, including research in tools and techniques that facilitate investigative and forensic work related to computer crimes. The Homeland Security Act of 2002 (§308) also authorizes the Undersecretary of Science and Technology of the Department of Homeland Security, when establishing university research centers, to consider universities with nationally recognized programs in information security. Although the Homeland Security Act of 2002 does not specifically call for research in this area, computer security makes up one of the portfolios of the Science and Technology Directorate.

Conclusion

Current Status. The roles and responsibilities of various federal departments and agencies in the area of computer security are relatively well defined. OMB and NIST are responsible for developing policy and standards, and for overseeing the implementation of those policies and standards, covering most of the federal government's computer systems. DOD, NSA, and the Director of Central Intelligence, working through the Committee on National Security Systems, are responsible for federal computer systems designated as national security systems. While inheriting the NCS and its responsibilities in the area of the NCS and telecommunications, the primary role of the Department of Homeland Security is to work with the private sector, state and local governments, and the public to protect the nation's information infrastructure (i.e. the Internet). The Secretary of Health and Human Services enforces regulations related to the privacy of individual health information held on private computer systems maintained by health care organizations. The SEC and other agencies with jurisdiction over financial institutions enforce regulations related to the privacy of individual financial information held on computer systems maintained by financial institutions. The SEC also enforces regulations related to the certification of internal financial controls (including those associated with a company's computer systems) for a large number of private sector firms. A number of agencies have the authority to investigate and prosecute federal computer crimes, in particular the Department of Justice and the

Secret Service (now part of DHS). NSA, NSF, NIST and DHS are specifically authorized to support research and development in computer security and to develop the nation's expertise in this area.

Issues. However, at least three issues have arisen concerning these roles and responsibilities: 1) the role the federal government in regulating the nation's privately owned and operated critical information infrastructure; 2) the relative roles of the Department of Homeland Security and the National Security Agency in setting policy and standards for computer and telecommunication systems handling critical infrastructure information; and, 3) the relative roles of the National Cyber Security Division and the National Communication System in setting policy and standards for dealing with the private sector.

Federal Regulation of the Private Sector. The current role of the federal government in regulating private sector computer systems is primarily derived from its interest to protect the privacy of individually identifiable information held on private computer systems or to improve the oversight of financial reporting by the private sector. Security of a company's or an individual's computer system or the Internet as a whole are not the policy objective. There is a long running debate about whether the federal government should take a more active regulatory role in improving private sector computer security. Two options that have been discussed include requiring the development of more secure computer software and/or requiring users to improve and maintain the security of their systems over time. A number of critics of the *National Strategy to Secure Cyberspace* have asserted that the Strategy did not go far enough in either of these directions in its recommendations.[5] These critics tend to come from the developers of security products and services. Both software developers and software users take the position that it is in a company's interest to sell and maintain secure products and systems and that market forces are the best way to ensure cost-effective security. Current policy is to engage the private sector and collaborate in efforts to raise awareness of security issues and to disseminate best practices.

Critical Infrastructure Information. The Homeland Security Act of 2002 defined a class of information called critical infrastructure information. Critical infrastructure information is information coming from the private sector, and state and local governments to the Department of Homeland Security concerning the identification of critical assets, their vulnerabilities, measures taken to protect them, and suspicious incidents. The Act gives the Secretary of Homeland Security authority to develop the information systems (as well as the protocols, etc.) needed to facilitate the sharing, storage, and analysis of this information. While not necessarily considered classified information, critical infrastructure information is considered sensitive and exempt from public disclosure. It might also be held and transmitted over systems that also handle classified or other types of sensitive information that would make the information systems handling it a national security

---

[5] For example, see, *White House Scales Back Cyberspace Plan.* The New York Times. February 14, 2003. [http://www.nytimes.com/2003/02/15/technology] . This website was last accessed on April 16, 2004. Also, *Bush's Cybersecurity Plan Falls Short, Report Says.* Computerworld. December 23, 2002. page 10.

system which falls within the jurisdiction of the Committee on National Security Systems and NSA. Who takes the lead in developing the policies and standards governing the systems being designed to handle this information?

Computer and Communication Security. Lastly, the Information Protection side of the Information Analysis and Infrastructure Protection Directorate at DHS has both a National Cyber Security Division and the National Communication System. As the technologies of telecommunications and computer become even more inextricable, there may appear to be some redundancies in the roles and responsibilities of these two entities. The role of the NCS is well established from over 40 years of experience. Its jurisdiction, while wide, still deals primarily with those assets considered necessary for national security related communications or during times of national emergencies. The NCSD has a much wider mandate; to work with all owners, operators, and users of the nation's information infrastructure. There is some debate about whether these two functions should merge or remain separate.