Calendar No. 489

106TH CONGRESS *2d Session*	SENATE	REPORT 106–259

GOVERNMENT INFORMATION SECURITY ACT OF 1999

REPORT

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1993

TO REFORM GOVERNMENT INFORMATION SECURITY BY STRENGTHENING INFORMATION SECURITY PRACTICES THROUGHOUT THE FEDERAL GOVERNMENT

APRIL 10, 2000.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

79–010 WASHINGTON : 2000

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

WILLIAM V. ROTH, JR., Delaware	JOSEPH I. LIEBERMAN, Connecticut
TED STEVENS, Alaska	CARL LEVIN, Michigan
SUSAN M. COLLINS, Maine	DANIEL K. AKAKA, Hawaii
GEORGE VOINOVICH, Ohio	RICHARD J. DURBIN, Illinois
PETE V. DOMENICI, New Mexico	ROBERT G. TORRICELLI, New Jersey
THAD COCHRAN, Mississippi	MAX CLELAND, Georgia
ARLEN SPECTER, Pennsylvania	JOHN EDWARDS, North Carolina
JUDD GREGG, New Hampshire	

HANNAH S. SISTARE, *Staff Director and Counsel*
ELLEN B. BROWN, *Senior Counsel*
SUSAN G. MARSHALL, *Professional Staff Member*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
DEBORAH COHEN LEHRICH, *Minority Counsel*
DARLA D. CASSELL, *Administrative Clerk*

Calendar No. 489

106TH CONGRESS, *2d Session* | SENATE | REPORT 106–259

GOVERNMENT INFORMATION SECURITY ACT OF 1999

APRIL 10, 2000.—Ordered to be printed

Mr. THOMPSON, from the Committee on Governmental Affairs, submitted the following

REPORT

[To accompany S. 1993]

The Committee on Governmental Affairs, to which was referred the bill (S. 1993) to reform Government information security by strengthening information security practices throughout the Federal Government, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends by voice vote that the bill as amended do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The Government Information Security Act would provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets. It is modeled on the "best practices" of leading organizations in the area of information security. It does this by strengthening responsibilities and procedures and coordinating information policy to ensure better control and oversight of systems. It also recognizes the highly networked nature of the current Federal computing environment and provides for governmentwide management and oversight of the related information security risks

including coordination of security efforts between civilian, national security and law enforcement communities.

S. 1993 would amend the Paperwork Reduction Act by inserting a new Subchapter II.

Agency Responsibilities: Agency heads would be responsible for developing and implementing security policies. This responsibility would be delegable to the agency's Chief Information Officer or comparable official. Each agency would be responsible for developing and implementing an agency-wide security program which must include risk assessment considering internal and external threats, risk-based policies, security awareness training for personnel, periodic reviews of the effectiveness of security policies including remedies to address deficiencies, and procedures for detecting, reporting and responding to security incidents. Further, each agency would be required to identify specific actions—including budget, staffing, and training resources—necessary to implement the security program and include this as part of its Government Performance and Results Act performance plan.

Director of OMB Responsibilities: The agency plans must be affirmatively approved by the Director of OMB who also would be responsible for establishing government-wide policies for the management of programs that support the cost-effective security of Federal information systems by promoting security as an integral part of each agency's business operations. Other responsibilities of the Director would include overseeing and coordinating agency implementation of security policies, and coordinating with the National Institute for Standards and Technology on the development of standards and guidelines for security controls for Federal systems. Such standards would be voluntary and consensus-based and developed in consultation with industry. To enforce agency accountability, the Director would be authorized to take budgetary action with respect to an agency's information resources management allocations. The OMB Director may delegate these responsibilities only down to the Deputy Director for Management.

Annual Audit: Based on the General Accounting Office's audit findings, S. 1993 adds a new requirement that each agency must annually undergo an independent evaluation of its information security program and practices to be conducted either by the agency's Inspector General, the General Accounting Office or an independent external auditor. GAO then will review these evaluations and report annually to Congress regarding the adequacy of agency information programs and practices.

National Security Systems: S. 1993 would require that the same management framework be applied to all systems including national security systems. However, in order to ensure that national security concerns are adequately addressed and that the appropriate individuals have oversight over national security and other classified information, the substitute amendment would vest responsibility for approving the security plan for these systems in the Secretary of Defense and the Director of Central Intelligence, rather than the Director of OMB. Additionally, for these systems, the Secretary of Defense or the Director of Central Intelligence shall designate who conducts the evaluation of these systems with the IG conducting an audit of the evaluation. Finally, the bill also al-

lows the defense and intelligence agencies to develop their own procedures for detecting, reporting and responding to security incidents.

Specific Agency Responsibilities:

The Department of Commerce would continue to be responsible for developing, issuing, reviewing and updating standards and guidance for the security of information in Federal computer systems.

The Department of Justice would be responsible for reviewing and updating guidance to agencies on legal remedies regarding security incidents and coordination with law enforcement agencies concerning such incidents.

The General Services Administration would be responsible for reviewing and updating guidance on addressing security considerations relating to the acquisition of information technology.

The Office of Personnel Management would be responsible for reviewing and updating regulations concerning computer security training for Federal civilian employees and for providing, along with the National Science Foundation, for personnel and training initiatives such as a Federal Cyber Service.

II. Background and Need for Legislation

Recent news accounts have described attacks on a handful of popular commercial Internet web sites. Less publicized, though potentially more damaging, is the fact that government computer systems also are vulnerable to the kinds of attacks these businesses have been suffering. Like the rest of the nation, government is increasingly dependent upon computers to store important information and perform vital tasks. That dependence, however, has not been accompanied by an equivalent growth in the security of those computer systems, leaving the government susceptible to potentially devastating disruptions in critical services, potentially exposing our citizens' most personal information and opening our national security apparatus to attack from terrorists or enemy states.

The Committee on Governmental Affairs has spent considerable time examining the security of the government's information technology systems. During the past several years, Committee hearings and Committee-requested reports from the General Accounting Office (GAO) have uncovered and publicly highlighted the security failures affecting our vulnerability to domestic and international cyberterrorism. On October 6, 1999, in testimony before the Senate Judiciary Committee, GAO noted that significant information security weaknesses exist in 22 Federal agencies it analyzed. In fact, GAO believes the problems in the government's information technology systems to be so severe that it has put governmentwide information security on its list of "high-risk" government programs.

GAO Reports

As a result of its work, GAO identified many specific weaknesses in agency controls and concluded that an underlying cause was inadequate security program planning and management. In particular, agencies were addressing identified weaknesses on a piece-

meal basis rather than proactively addressing systemic causes that diminished security effectiveness throughout the agency.

Over the years, the following GAO reports provided the Committee with substantial evidence of Federal agency vulnerabilities in the area of information security and became the basis for S. 1993:

Department of Energy Procedures Lacking to Protect Computerized Data (GAO/AIMD–95–118, June 1995): Allegations were made that the Idaho National Engineering Laboratory sold surplus computer equipment that contained sensitive data to an Idaho businessman. GAO concluded that some of the computers sold may have contained sensitive data, but did not determine how many. GAO added that, like all Federal agencies, the Department of Energy is required to establish computer security safeguards, yet it had not.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD–96–84, May 1996): Unknown and unauthorized individuals were increasingly attacking and gaining access to highly sensitive unclassified information at the DoD. These attacks ranged from being nuisances to being a serious threat to national security. According to GAO, DoD needed to make better use of technology and, more importantly, needed to develop better policies and employ better trained personnel.

Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD–96–110, September 1996): GAO provided OMB with a number of recommendations on how to better manage governmentwide information technology system security. The recommendations included directing the Office of Information and Regulatory Affairs, Office of Federal Financial Management and others to review Chief Financial Officer audits for any information security weaknesses, proactively monitoring agency information security effectiveness through reviews, and encouraging the development of improved information resources to better evaluate agency information security effectiveness.

Resolving Serious Information Security Weaknesses (GAO/HR–97–1, February 1997): GAO identified information security as a governmentwide high-risk area because of growing evidence indicating that controls over computer operations were not effective. GAO recommended that agencies proactively manage risk and that strong, governmentwide leadership be provided on the issue by OMB in order to ensure that executives understand their risks, monitor agency performance, and resolve issues affecting multiple agencies.

IRS Systems: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD–97–76, April 1997): The GAO reported that "weaknesses in IRS computer security controls continue to place IRS's automated systems and taxpayer data at serious risk to both internal and external attack." The report stated that more needs to be done at IRS to combat the unauthorized access or browsing of taxpayer records by agency employees. For example, the GAO found that IRS's ability to detect and monitor employee browsing of taxpayer data remains limited. In addition, unauthorized employees were given access to sensitive computer areas while employees whose jobs did not require it were given the

ability to change, alter, or delete taxpayer data. Additionally, the GAO reported that the IRS could not account for a total of 397 missing computer tapes (some of which contained sensitive taxpayer data or privacy information) and found that tapes and disks containing taxpayer data were not erased prior to reuse (thus potentially allowing unauthorized access to sensitive data).

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD–98–145, May 1998): To determine the extent to which the State Department's systems are vulnerable to unauthorized attack, the GAO directed and supervised penetration testing of State Department systems. GAO's reviews and testing revealed the susceptibility of the State Department's systems to unauthorized access and that unauthorized retrieval of sensitive information from such systems was possible. Specifically, testers were able to download, delete, and modify data, add new data, shut down servers, and monitor network traffic. Moreover, this activity went largely undetected, further underscoring the State Department's serious vulnerability to attack.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD–98–155, May 1998): Malicious attacks on computer systems could cause nationwide disruption of air traffic or even the loss of life due to collisions. Such attacks are an increasing threat to the Federal Aviation Administration's (FAA) systems and, consequently, those who fly. Auditors at GAO found that, in all critical areas of review, FAA was ineffective in implementing sound computer security practices. In fact, FAA was found not only to be ineffectively managing current systems, but it did not provide accurate security specifications in new modernization efforts.

Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD–99–47, May 1999): GAO conducted an evaluation of the National Aeronautics and Space Administration's (NASA) information technology security program to determine (1) whether NASA's mission critical systems are vulnerable to unauthorized access; (2) whether NASA is effectively managing its information systems security; and (3) what NASA is doing to address the risk of unauthorized access to mission critical systems. GAO determined that NASA's information security program did not include key elements of a comprehensive information technology security management program because it did not assess risks, effectively implement controls, provide training, monitor policy compliance, or provide incident response capabilities.

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD–98–92, September 1998): GAO conducted a review of 24 of the largest Federal agencies and found serious weaknesses in the government's ability to adequately protect: (1) federal assets from fraud and misuse; (2) sensitive information from inappropriate disclosure; and (3) critical operations, including some affecting safety, from disruption. According to the report's conclusions, these weaknesses place critical government operations, such as national defense, tax collection, law enforcement and benefit distribution, at risk.

Further, the Committee asked GAO to study organizations with superior information security programs to identify management practices that could benefit Federal agencies. This report detailed

the "best practices" used by these organizations and became the basis for the management framework of S. 1993:

Information Security Management: Learning from Leading Organizations (GAO/AIMD–98–68, May 1998): At the Committee's request, GAO studied the management practices of eight organizations known for their superior security programs and found that these organizations managed information security through continuous management activities which incorporated specific practices to support their information security principles. These practices included providing senior management support and involvement, defining procedures, integrating business and technical experts, holding business units responsible, documenting and maintaining results, identifying threats, ranking critical assets, estimating potential damage, identifying cost-effective mitigating controls, and documenting assessment findings.

III. Legislative History

The oversight of Federal government information management is within the jurisdiction of the Committee on Governmental Affairs. Over the years, the Committee spent considerable time on this issue. During the 105th Congress, Committee hearings focused on information security and cyberterrorism. The Committee uncovered and identified failures of information security affecting our international security and revealing our vulnerability to domestic and international terrorism. These hearings highlighted our nation's vulnerability to computer attacks—from international and domestic terrorists to crime rings to everyday hackers—and led to the development of S. 1993.

HEARINGS

On May 18, 1998, the Committee held a hearing—"Weak Computer Security in the Government: Is the Public at Risk?"—on how Federal agencies are providing computer security. The hearing provided many new insights into how the government has not kept pace with the advances in technology and its multiple applications. In fact, the hearing revealed that, not only has technology advanced, it has become less complex for users and its availability is not limited and instead is widely distributed around the world.

Witnesses at this hearing addressed systemic problems which make government computer and communication systems vulnerable to both deliberate and inadvertent attacks. Dr. Peter Neumann, Principal Scientist, Computer Science Laboratory, SRI International, testified that our nation's underlying information infrastructure (for example, power generation, transmission and distribution, air traffic control, and telecommunications) remains at risk. Even though the risk is widely known, Dr. Neumann stated that until high-visibility disasters occur, few people are willing to admit that something drastic needs to be done. He testified that it may take a Chernobyl-scale event to raise awareness levels adequately. Also, seven members of L0pht, a "hacker" think tank, provided testimony to the Committee. L0pht said that, in a matter of thirty minutes, they could unlock the security systems within the Internet and make the entire system unusable for a couple of days.

On June 24, 1998, the Committee held another hearing—"Cyber Attack: Is the Nation at Risk?" This hearing addressed threats and vulnerabilities to the U.S. national security due to weak computer security.

The Director of Central Intelligence, Mr. George Tenet, testified that information warfare has the potential to deal a crippling blow to our national security if strong measures are not taken to counter it. Director Tenet noted that the U.S. is highly dependent on information systems and therefore is the most likely target for an information-based attack. He testified that potential threats range from national intelligence and military organizations to terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders. Director Tenet stated that several countries, including, Russia and China, have government-sponsored information warfare programs with both offensive and defensive applications. These countries see information warfare as a way of leveling the playing field against a stronger military power, such as the U.S. The more difficult threat to assess is that from non-State actors, such as terrorists and criminals. Cyber attacks offer these groups greater security and operational flexibility. They can launch an assault from almost anywhere in the world without directly exposing themselves to physical harm.

The Director of the National Security Agency (NSA), Lieutenant General Kenneth Minihan, USAF, testified on the findings from the DoD's exercise "Eligible Receiver." This exercise demonstrated that our nation's information infrastructure is riddled with vulnerabilities and that severe deficiencies exist in our ability to respond to a coordinated attack on our national infrastructure and information systems. During the exercise, a team of hackers from NSA, using tools easily obtained from the Internet, proved that they could deny our military the ability to deploy forces and conduct operations.

On September 23, 1998, the Committee held a hearing on computer security in Federal government agencies which examined whether private information held by the Federal government—information relating to one's identification, finances and health—is susceptible to unauthorized access and manipulation by computer hackers. The hearing focused on the results of penetration testing performed under GAO's direction and supervision at two federal agencies—the Department of Veterans Affairs (VA) and the Social Security Administration (SSA).

The Committee heard testimony from agents of the SSA Office of Inspector General who described a variety of computer crimes committed by SSA employees. The agents discussed in detail a series of prosecutions, known as "Operation Pinch," in which 14 SSA employees were convicted for their part in a widespread credit card fraud ring centered in New York. The agents determined that SSA employees sold identity information on 20,000 people whose credit cards then were fraudulently activated by a West African crime ring, resulting in bank losses of at least $70 million. "Operation Pinch" demonstrated the danger of the "inside threat" to agencies that do not adequately monitor and limit access to computer information by their own employees.

Witnesses from GAO described the results of penetration testing at the VA and SSA. GAO would have been able, during its VA testing, to alter, disclose or delete sensitive information, such as financial data and personal information on veterans' medical records and benefit payments. GAO's penetration went undetected because the VA did not have a monitoring system. GAO's penetration testing of the SSA exposed vulnerabilities in the SSA computer system to both external and internal intrusions. These types of weakness place at risk private information held by SSA, including Social Security numbers, earnings, and benefits.

LEGISLATION

S. 1993, the Government Information Security Act, was introduced on November 19, 1999, by Senator Thompson (for himself and Senator Lieberman). Senators Abraham, Voinovich, Akaka, Cleland, Collins, and Stevens became additional co-sponsors.

On March 2, 2000, the Committee held a legislative hearing on S. 1993. The Committee sought general comments on S. 1993 and additional testimony on the security of Federal information systems including computer system vulnerabilities, how people exploit those weaknesses and what Federal agencies should be doing to strengthen the management of information systems. The following witnesses presented testimony on S. 1993: Mr. Kevin Mitnick, a self-described reformed hacker; Mr. Jack Brock, Director, Governmentwide and Defense Information Systems, General Accounting Office; Ms. Roberta Gross, Inspector General, National Aeronautics and Space Administration; Mr. James Adams, Chief Executive Officer, iDefense; and Mr. Ken Watson, Manager, Critical Infrastructure, Cisco Systems.

Mr. Mitnick provided testimony which outlined four components of information security: physical security, network security, computer systems security, and personnel security. After detailing the first three elements, Mr. Mitnick highlighted the most complex element of information security—personnel security—noting that weaknesses in personnel security negate the effort and cost of the other three types of security efforts. He said, "The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption, and secure access devices and it is money wasted because none of these measures address the link in the security chain, the people who use, administer, operate and account for computer systems that contain protected information."

Mr. Mitnick's testimony provided the Committee with examples of how all of the elements of information security can be compromised. He explained to the Committee how he successfully tricked the employees of a multi-national company into giving him pass codes to the company's security access devices. Mr. Mitnick characterized S. 1993 as a good first step toward the goal of increasing information security for government systems and recommended increased oversight, education and training.

Mr. James Adams provided testimony supporting S. 1993. He said, "By stepping up to the plate and tackling computer security with an innovative, bold approach the Thompson-Lieberman bill significantly boosts the chances of reversing the current bureau-

cratic approach to a dynamic problem." His testimony focused on current threats and vulnerabilities within the nation's critical infrastructure and his belief that total cultural reform is needed. One of Mr. Adams's proposals for reform included the establishment of a Business Assurance Office to better manage governmentwide information security. This Office would draw on the skills of individuals such as Chief Information Officers, Chief Financial Officers, and Chief Security Officers, in order for policies to be devised which take into account the whole environment of a public sector organization.

Mr. Watson's testimony focused on "best practices" and the management approach applied within Cisco Systems. For example, Mr. Watson highlighted the need for a continuous management approach which includes assessing information, determining the level of risk of exposure of that data, and applying the appropriate solutions. Mr. Watson emphasized that each Federal agency and department should execute its own programs based on tailored mission and risk analyses because no two departments will have the same requirements at the same time. And those requirements and solutions will change over time.

During the hearing Senator Thompson said, "Hopefully the recent breaches of security at the various dot.com companies is the wake up call needed to focus attention on the security of government computer systems. We know that federal agencies continue to use a band-aid approach to computer security rather than addressing the systemic problems which make government systems vulnerable to repeated computer attacks." Senator Lieberman said, "The security of our digital information is something that affects every one of us on a daily basis and should be taken as seriously as the security of our property, of our neighborhoods, of our communities, of our Nation, and in the worst case, as seriously as the security of our lives * * * the intention of the bill is to raise up computer security as a priority consideration for Federal agencies and individual Federal employees who have responsibility."

COMMITTEE ACTION

The Committee considered a substitute amendment to S. 1993 offered by Chairman Thompson, on behalf of himself and Senator Lieberman, at a business meeting on March 23, 2000. The Thompson/Lieberman substitute included changes made based on comments received from the witnesses at the hearing held on March 2, 2000, and working with the Office of Management and Budget, the agency Inspectors General, the Department of Defense and others in the intelligence community, and industry.

The substitute amendment requires that the same management framework be applied to all systems including national security systems. However, in order to ensure that national security concerns were adequately addressed and that the appropriate individuals have oversight over national security information, the substitute amendment vests responsibility for approving the security plan for these systems in the Secretary of Defense and the Director of Central Intelligence, rather than the Director of OMB. Additionally, for these systems, the Secretary of Defense or the Director of Central Intelligence shall designate who conducts the evaluation of

these systems, with the IG conducting an audit of the evaluation. Finally, the amendment also allows defense and intelligence agencies to develop their own procedures for detecting, reporting and responding to security incidents. And, it gives the Director of the Office of Management and Budget and agency heads the discretion to apply more stringent policies and procedures where appropriate for systems critical to the missions of Federal agencies.

In addition, the amendment includes language which the Committee intends to lay the foundation for the education and training of a Federal Cyber Service. As envisioned under the President's National Plan for Information Systems Protection, the Committee intends that the program will, at a minimum, provide for a ROTC-like scholarships-for-service program to get educated information security professionals straight from their university training into government service.

Finally, by unanimous consent, the Committee added language on behalf of Senator Akaka to require agencies to identify specific actions necessary to implement the security program and include this as part of the agency's Government Performance and Results Act performance plan. These actions include budget, staffing and training requirements and could include specific funding necessary to perform the independent evaluation.

The Committee passed the Thompson/Lieberman substitute amendment by voice vote and voted to report it to the full Senate. Senators present were: Thompson, Collins, Stevens, Domenici, Cochran, Voinovich, Lieberman, Akaka, and Cleland.

IV. SECTION-BY-SECTION

SECTION 1. SHORT TITLE

This section states the short title of the bill.

SECTION 2. COORDINATION OF FEDERAL INFORMATION POLICY

This section would add a new subchapter II to chapter 35 of title 44, United States Code, which currently contains the information resources management requirements of the Paperwork Reduction Act. The new subchapter II, entitled "Information Security," would establish comprehensive and coordinated information security requirements for Federal agencies to be implemented under the guidance of the Office of Management and Budget (OMB), the Secretary of Defense and the Director of Central Intelligence. It also would coordinate information security provisions under the new subchapter II with other information resources management requirements in title 44 and other laws.

The new subchapter II would add sections 3531 through 3535 to title 44, as follows:

Section 3531. Purposes

This section would establish as the purposes of subchapter II:

(1) providing a comprehensive framework for managing the security of information resources that support Federal operations and assets;

(2) assuring that implementation of improved security management measures does not adversely affect opportunities for

interoperability in the Federal computing environment, and providing effective governmentwide management and oversight of information security risks and coordination of information security efforts;

(3) establishing minimum controls to protect Federal information and information systems; and

(4) improving oversight of Federal agency information security programs.

Section 3532. Definitions

(a) This section would apply to subchapter II the definitions now contained in the Paperwork Reduction Act, except that—

(b)(1) the term "information technology" would be defined by section 5002 of the Clinger-Cohen Act (40 U.S.C. 1401); and

(2) the term "mission critical system" would be defined as (A) a national security system pursuant to section 5142 of the Clinger-Cohen Act; (B) a system that is protected as secret at all times by procedures established by an Executive Order or an Act of Congress in the interest of national defense or foreign policy; or (C) a system which processes information, the loss, misuse, disclosure, unauthorized access to or modification of which would have a debilitating impact on an agency's mission.

Section 3533. Authority and functions of the Director

This section would prescribe the authority and functions of the Director of OMB with respect to information security.

Subsection 3533(a) would require the Director to establish governmentwide policies for the management of programs that support the cost-effective security of government information systems by promoting security as an integral part of agency business operations, including information technology architectures. The policies would require a continuing cycle of risk management to include risk assessments, implementation of controls to address risks, promotion of continuing awareness of risks, and continual monitoring and evaluation of information security policies and practices.

Subsection 3533(b) would include within the Director's authority under subsection (a)—

(1) overseeing and developing policies to implement agency responsibilities under applicable law to ensure the privacy, confidentiality, and security of Federal information;

(2) requiring agencies to develop information security protections that are commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, disruption, modification, or destruction of information and consistent with specified provisions of law;

(3) directing agency heads to (A) identify, use, and share best security practices; (B) develop an agency-wide information security plan; (C) incorporate information security principles and practices throughout the agency's information systems' life cycles; and (D) ensure that the agency's information security plan is practiced throughout all agency information systems' life cycles;

(4) overseeing the development and implementation of standards relating to Federal computer system security controls by

the Commerce Department's National Institute of Standards and Technology (NIST);

(5) overseeing and coordinating compliance with this section in a manner consistent with the Freedom of Information Act, the Privacy Act, and other information management laws; and

(6) taking any authorized action under 40 U.S.C. section 1413(b)(5) which the Director considers appropriate, including budget or appropriations-related actions, to enforce the accountability of agency heads for information resources management, including the requirements of this subchapter and information technology investments.

Subsection 3533(c) would limit delegation of the Director's authority under this section to the Director of Central Intelligence and the Secretary of Defense for systems identified under (A) and (B) of section 3532(b)(2) and to the OMB Deputy Director for Management for all other systems.

Section 3534. Federal agency responsibilities

Subsection (a)(1) of this section would assign agency heads responsibility for: (A) ensuring the integrity, confidentiality, authenticity, availability, and non-repudiation of the information in their systems; (B) adopting information security policies, procedures, and control techniques commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, disruption, modification, or destruction of information; and (C) ensuring that the agency's information security plan is practiced throughout each system's life cycle.

Subsection (a)(2) would ensure that the appropriate senior agency officials are responsible for: (A) assessing information security risks associated with the operations and assets for programs and systems over which such officials have control; (B) determining appropriate levels of information security for the operations and assets; and (C) periodically testing and evaluating information security controls and techniques.

Subsection (a)(3) would require agency heads to delegate administration of all functions under subchapter II to the agency's Chief Information Officer (CIO), or a comparable official if the agency does not have a CIO. These functions include (A) designating a senior agency information security official who would report back to the CIO or comparable official; (B) developing and maintaining an agencywide information security program; (C) ensuring that the agency effectively implements and maintains information security policies, procedures and control techniques; (D) training and overseeing personnel with information security responsibilities; and (E) assisting senior agency officials with their responsibilities under paragraph (2).

Subsection (a)(4) would require agency heads to ensure that the agency has sufficiently trained personnel to assist in complying with subchapter II and related administrative requirements.

Subsection (a)(5) would require agency heads to ensure that the CIO, in coordination with senior agency officials, periodically evaluates the effectiveness of the agency's information security program, including testing control techniques; implements appropriate remedial actions based on those evaluations; and reports to the agency

head on the results of tests and evaluations and the progress of remedial actions.

Subsection 3534(b) would require each agency to develop and implement an agencywide information security program. The program would include: (A) periodic risk assessments; (B) policies and procedures that cost-effectively reduce risks to an acceptable level and ensure compliance with subchapter II and related requirements; (C) security awareness training; (D) periodic management testing and evaluation of the effectiveness of security policies and procedures and a process for remedying significant deficiencies; and (E) procedures for detecting, reporting, and responding to security incidents for all systems including a separate process for systems identified under (A) and (B) of section 3532(b)(2). Each information security program would be subject to the approval of the OMB Director, or the Secretary of Defense or Director, Central Intelligence (in the case of systems identified under (A) and (B) of section 3532(b)(2)) and would be reviewed at least annually by agency program officials in consultation with the CIO.

Subsection 3534(c) would require agencies to examine the adequacy and effectiveness of information security policies, procedures, and practices in their plans and reports relating to their annual budget, information resources management under the Paperwork Reduction Act, the Clinger-Cohen Act, the Government Performance and Results Act, and financial management laws. Any significant deficiency would be reported as a material weakness under the applicable reporting requirement.

Section 3535. Annual independent evaluation

This section would require each agency to obtain annually an independent evaluation of its information security program and practices. The evaluation would include an assessment of compliance with subchapter II and related requirements as well as tests of the effectiveness of information security control techniques. The evaluator conducting the evaluation may use the results of other audits or evaluations relating to agency programs or practices.

The annual evaluation would be performed by the agency Inspector General or by an independent evaluator determined by the Inspector General. An agency that does not have an Inspector General would contract with an independent evaluator for the annual evaluation. A General Accounting Office (GAO) evaluation may be used in lieu of the evaluation under this section.

In the case of systems described in paragraphs (A) and (B) of section 3532(b)(2), the evaluation required under the section, shall be performed only by an entity designated by the Secretary of Defense or the Director of Central Intelligence, as appropriate and, an audit of the evaluation shall be performed by the Inspector General.

The results of the annual evaluation or audit (in the case of systems identified under (A) or (B) of section 3532(b)(2)) would be submitted to OMB within one year of enactment of this Act and on that date every year thereafter.

The GAO would annually review the evaluations required under this section or an audit of the evaluation in the case of systems described in paragraphs (A) and (B) of section 3532(b)(2) and other

information security evaluation results, and report to Congress on the adequacy of agency information programs and practices.

Consistent with applicable law and commensurate with risk, agencies and evaluators would protect information from disclosure if such disclosure would adversely affect information security.

SECTION 3. RESPONSIBILITIES OF CERTAIN AGENCIES

This section would assign responsibilities to specified Federal agencies as follows:

Department of Commerce

Subsection (a) provides that the National Institute of Standards and Technology, with requested or required technical assistance from the National Security Agency shall (except as provided in subsection (b))—

(1) establish standards and guidance for the security of information in Federal computer systems, including methods and techniques for security systems and validation programs;

(2) establish guidelines for training in computer security awareness and practices, with assistance from the Office of Personnel Management (OPM);

(3) provide guidance to agencies on security planning;

(4) provide guidance and assistance to agencies on cost-effective controls when interconnecting with other systems; and

(5) evaluate information technologies to assess and alert agencies to security vulnerabilities as soon as possible.

Department of Defense and the Intelligence Community

Subsection (b) provides that the Secretary of Defense and the Director of Central Intelligence shall (notwithstanding section 2 of this Act), consistent with their respective authorities—

(1) develop and issue information security policies, standards and guidelines for systems described in paragraphs (A) and (B) of subsection 3532(b)(2) that provide more stringent protection than policies, principles, standards, and guidelines required under section 2 of this Act, as amended; and

(2) ensure the implementation of information security policies, principles, standards, and guidelines as prescribed by subsection (1).

Department of Justice

Subsection (c) would require the Justice Department to review and update guidance to agencies on: (1) legal remedies regarding security incidents and ways to work with law enforcement agencies concerning such incidents; and (2) lawful uses of security techniques and technologies.

General Services Administration

Subsection (d) would require the General Services Administration to: (1) assist agencies in fulfilling their responsibilities under section 3534(b)(2)(E) and in acquiring cost-effective security products, services, and incident response capabilities.

Office of Personnel Management

Subsection (e) would require the Office of Personnel Management to: (1) review and update its regulations on computer security training and (2) assist the Commerce Department in updating and maintaining guidelines for training in computer security awareness and best practices and (3) work with the National Science Foundation in providing agencies with the appropriate personnel and training initiatives, including scholarships and fellowships to ensure that the Federal government has adequate sources of information security training and education and qualified personnel.

Subsection (f) would require that, notwithstanding any provision in this Act, the Secretary of Defense and the Director of Central Intelligence shall develop policies, principles, procedures and guidelines for mission critical systems subject to their control, and these policies may be adopted by the Director of OMB, or by an agency head, as appropriate, to the mission critical systems of all agencies or of that agency if consistent with other OMB and Commerce Department guidance. Further, agencies may use the more stringent policies, principles, procedures and guidelines for any information system if consistent with other OMB and Commerce Department guidance.

SECTION 4. TECHNICAL AND CONFORMING AMENDMENTS

This section would make technical and conforming changes to chapter 35 of title 44, United States Code.

SECTION 5. EFFECTIVE DATE

This section would provide for the bill to become effective 30 days after the date of its enactment into law.

V. Regulatory Impact Statement

Paragraph 11(b)(1) of the Standing Rules of the Senate requires that each report accompanying a bill evaluate "the regulatory impact which would be incurred in carrying out this bill."

The enactment of this legislation will not have significant regulatory impact. S. 1993 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would have no impact on state, local or tribal governments.

VI. CBO Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, March 29, 2000.

Hon. Fred Thompson,
Chairman, Committee on Governmental Affairs,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1993, the Government Information Security Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is John R. Righter.

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

S. 1993—Government Information Security Act

S. 1993 would require federal agencies to perform certain tasks to improve the security of their computer systems. Subject to the availability of appropriated funds, CBO estimates that implementing S. 1993 would cost federal agencies between $10 million and $15 million annually to audit their security programs and practices. While this work should both increase the cost-effectiveness of federal security systems and reduce the likelihood of costly service disruptions, CBO has no basis for estimating the amount of potential savings from such improvements.

The bill would not affect direct spending or receipts, so pay-as-you-go procedures would not apply. S. 1993 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

S. 1993 would require federal agencies to develop a risk-based program for ensuring the security of their information systems, including designating a senior official to oversee the program, periodically assessing and testing their systems, and providing training to personnel. In addition, the bill would require that either an inspector general or independent evaluator annually audit an agency's security programs and practices. S. 1993 also would specify the responsibilities of particular agencies in securing the government's information systems, including the National Institute of Standards and Technology, the Department of Justice, and the General Services Administration. Finally, the bill would require the Office of Management and Budget (OMB) to establish policies for implementing its provisions.

Most of S. 1993 would codify and centralize current practice, including directions provided in the Government Security Act, OMB Circular No. A–130 (Management of Federal Information Resources), and Presidential Decision Directive 63, concerning the protection of critical infrastructure. While some agencies already evaluate portions of their information systems through the financial audits required by the Chief Financial Officers (CFO) Act and the security reviews required by OMB Circular No. A–130, the bill would call for agencies to audit their systems more extensively and regularly.

Based on information from the General Accounting Office, which has reviewed the security practices of federal agencies, and OMB, CBO estimates that requiring the annual audits would increase agency costs by between $10 million and $15 million annually, subject to the availability of appropriated funds. That estimate assumes that the 25 largest federal departments and agencies those with appointed CFOs) would regularly test the general and management controls of critical, nonfinancial operations. We estimate that the evaluation of between 55 and 75 computer systems oper-

ated by these agencies would cost around $150,000 each, or a total of around $10 million annually. Although much uncertainty exists as to the number and complexity of computer operations that smaller agencies would need to evaluate, as well as the extent that such evaluations already take place, CBO expects that applying the audit requirement to them would increase the provision's cost by as much as 50 percent.

In addition, the audits should both improve the cost-effectiveness of federal security systems and decrease the likelihood of costly service disruptions. CBO, however, cannot estimate the amount of potential savings from such improvements.

The CBO staff contact is John R. Righter. This estimate was approved by Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

VII. CHANGES TO EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows, (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman).

UNITED STATES CODE

TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

SUBCHAPTER I—FEDERAL INFORMATION POLICY

SUBCHAPTER II—INFORMATION SECURITY

Subchapter I—Federal Information Policy

§ 3501. Purposes

The purposes of this [chapter] *subchapter* are to—

* * * * * * *

(11) improve the responsibility and accountability of the Office of Management and Budget and all other Federal agencies to Congress and to the public for implementing the information collection review process, information resources management, and related policies and guidelines established under this [chapter] *subchapter.*

§ 3502. Definitions

As used in this [chapter] *subchapter-*

* * * * * * *

§ 3503. Office of Information and Regulatory Affairs

* * * * * * *

(b) There shall be at the head of the Office an Administrator who shall be appointed by the President, by and with the advice and consent of the Senate. The Director shall delegate to the Administrator the authority to administer all functions under this [chapter] *subchapter*, except that any such delegation shall not relieve the Director of responsibility for the administration of such functions. The Administrator shall serve as principal adviser to the Director on Federal information resources management policy.

§ 3504. Authority and functions of Director

(a)(1) The Director shall oversee the use of information resources to improve the efficiency and effectiveness of governmental operations to serve agency missions, including burden reduction and service delivery to the public. In performing such oversight, the Director shall—

(A) develop, coordinate and oversee the implementation of Federal information resources management policies, principles, standards, and guidelines; and

(B) provide direction and oversee—

(i) the review and approval of the collection of information and the reduction of the information collection burden;

(ii) agency dissemination of and public access to information;

(iii) statistical activities;

(iv) records management activities;

(v) privacy, confidentiality, security, disclosure, and sharing of information; and

(vi) the acquisition and use of information technology.

(2) The authority of the Director under this [chapter] *subchapter* shall be exercised consistent with applicable law.

* * * * * * *

(d) With respect to information dissemination, the Director shall develop and oversee the implementation of policies, principles, standards, and guidelines to—

(1) apply to Federal agency dissemination of public information, regardless of the form or format in which such information is disseminated; and

(2) promote public access to public information and fulfill the purposes of this [chapter] *subchapter,* including through the effective use of information technology.

* * * * * * *

(f) With respect to records management, the Director shall—

(1) provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination in the administration of chapters 29, 31, and 33 of this title with the information resources management policies, principles, standards, and guidelines established under this [chapter] *subchapter;*

* * * * * * *

§ 3505. Assignment of tasks and deadlines

(a) In carrying out the functions under this [chapter] *subchapter,* the Director shall—

(1) in consultation with agency heads, set an annual Governmentwide goal for the reduction of information collection burdens by at least 10 percent during each of fiscal years 1996 and 1997 and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001, and set annual agency goals to—

(A) reduce information collection burdens imposed on the public that—

(i) represent the maximum practicable opportunity in each agency; and

(ii) are consistent with improving agency management of the process for the review of collections of information established under section 3506(c); and

(B) improve information resources management in ways that increase the productivity, efficiency and effectiveness of Federal programs, including service delivery to the public;

(2) with selected agencies and non-Federal entities on a voluntary basis, conduct pilot projects to test alternative policies, practices, regulations, and procedures to fulfill the purposes of this [chapter] *subchapter,* particularly with regard to minimizing the Federal information collection burden; and

* * * * * * *

§ 3506. Federal agency responsibilities

(a)(1) The head of each agency shall be responsible for—

(A) carrying out the agency's information resources management activities to improve agency productivity, efficiency, and effectiveness; and

(B) complying with the requirements of this [chapter] *subchapter* and related policies established by the Director. (2)(A) Except as provided under subparagraph (B), the head of each agency shall designate a senior official who shall report directly to such agency head to carry out the responsibilities of the agency under this [chapter] *subchapter*.

(B) The Secretary of the Department of Defense and the Secretary of each military department may each designate senior officials who shall report directly to such Secretary to carry out the responsibilities of the department under this [chapter] *subchapter*. If more than one official is designated, the respective duties of the officials shall be clearly delineated.

(3) The senior official designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this [chapter] *subchapter*, including the reduction of information collection burdens on the public. The senior official and employees of such office shall be selected with special attention to the professional qualifications required to administer the functions described under this [chapter] *subchapter*.

* * * * * * *

(4) in consultation with the Director, the Administrator of General Services, and the Archivist of the United States, maintain a current and complete inventory of the agency's information resources, including directories necessary to fulfill the requirements of section 3511 of this [chapter] *subchapter*; and

(5) in consultation with the Director and the Director of the Office of Personnel Management, conduct formal training programs to educate agency program and management officials about information resources management.

(c) With respect to the collection of information and the control of paperwork, each agency shall—

(1) establish a process within the office headed by the official designated under subsection (a), that is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved under this [chapter] *subchapter*, to—

(A) review each collection of information before submission to the Director for review under this [chapter] *subchapter*, including—

* * * * * * *

§ 3507. Public information collection activities; submission to Director; approval and delegation

* * * * * * *

(e)(1) Any decision by the Director under subsection (c), (d), (h), or (j) to disapprove a collection of information, or to instruct the agency to make substantive or material change to a collection of in-

formation, shall be publicly available and include an explanation of the reasons for such decision.

(2) Any written communication between the Administrator of the Office of Information and Regulatory Affairs, or any employee of the Office of Information and Regulatory Affairs, and an agency or person not employed by the Federal Government concerning a proposed collection of information shall be made available to the public.

(3) This subsection shall not require the disclosure of—

(A) any information which is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; or

(B) any communication relating to a collection of information which is not approved under this [chapter] *subchapter*, the disclosure of which could lead to retaliation or discrimination against the communicator.

* * * * * * *

(h)(1) If an agency decides to seek extension of the Directors approval granted for a currently approved collection of information, the agency shall—

(A) conduct the review established under section 3506(c), including the seeking of comment from the public on the continued need for, and burden imposed by the collection of information; and

(B) after having made a reasonable effort to seek public comment, but no later than 60 days before the expiration date of the control number assigned by the Director for the currently approved collection of information, submit the collection of information for review and approval under this section, which shall include an explanation of how the agency has used the information that it has collected.

(2) If under the provisions of this section, the Director disapproves a collection of information contained in an existing rule, or recommends or instructs the agency to make a substantive or material change to a collection of information contained in an existing rule, the Director shall—

(A) publish an explanation thereof in the Federal Register; and

(B) instruct the agency to undertake a rulemaking within a reasonable time limited to consideration of changes to the collection of information contained in the rule and thereafter to submit the collection of information for approval or disapproval under this [chapter] *subchapter*.

(3) An agency may not make a substantive or material modification of a collection of information after such collection has been approved by the Director, unless the modification has been submitted to the Director for review and approval under this [chapter] *subchapter*.

* * * * * * *

(j)(1) The agency head may request the Director to authorize a collection of information, if an agency head determines that—

(A) a collection of information—

(i) is needed prior to the expiration of time periods established under this [chapter] *subchapter*; and

(ii) is essential to the mission of the agency; and

(B) the agency cannot reasonably comply with the provisions of this [chapter] *subchapter* because—

(i) public harm is reasonably likely to result if normal clearance procedures are followed;

(ii) an unanticipated event has occurred; or

(iii) the use of normal clearance procedures is reasonably likely to prevent or disrupt the collection of information or is reasonably likely to cause a statutory or court ordered deadline to be missed.

(2) The Director shall approve or disapprove any such authorization request within the time requested by the agency head and, if approved, shall assign the collection of information a control number. Any collection of information conducted under this subsection may be conducted without compliance with the provisions of this [chapter] *subchapter* for a maximum of 90 days after the date on which the Director received the request to authorize such collection.

* * * * * * *

§ 3509. Designation of central collection agency

The Director may designate a central collection agency to obtain information for two or more agencies if the Director determines that the needs of such agencies for information will be adequately served by a single collection agency, and such sharing of data is not inconsistent with applicable law. In such cases the Director shall prescribe (with reference to the collection of information) the duties and functions of the collection agency so designated and of the agencies for which it is to act as agent (including reimbursement for costs). While the designation is in effect, an agency covered by the designation may not obtain for itself information for the agency which is the duty of the collection agency to obtain. The Director may modify the designation from time to time as circumstances require. The authority to designate under this section is subject to the provisions of section 3507(f) of this [chapter] *subchapter*.

* * * * * * *

§ 3512. Public protection

(a) Notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information that is subject to this [chapter] *subchapter* if—

(1) the collection of information does not display a valid control number assigned by the Director in accordance with this [chapter] *subchapter*;

* * * * * * *

§ 3514. Responsiveness to Congress

(a)(1) The Director shall—

(A) keep the Congress and congressional committees fully and currently informed of the major activities under this [chapter] *subchapter*; and

(B) submit a report on such activities to the President of the Senate and the Speaker of the House of Representatives annually and at such other times as the Director determines necessary.

(2) The Director shall include in any such report a description of the extent to which agencies have—

(A) reduced information collection burdens on the public, including—

(i) a summary of accomplishments and planned initiatives to reduce collection of information burdens;

(ii) a list of all violations of this [chapter] *subchapter* and of any rules, guidelines, policies, and procedures issued pursuant to this [chapter] *subchapter*;

* * * * * * *

§ 3515. Administrative powers

Upon the request of the Director, each agency (other than an independent regulatory agency) shall, to the extent practicable, make its services, personnel, and facilities available to the Director for the performance of functions under this [chapter] subsection.

§ 3516. Rules and regulations

The Director shall promulgate rules, regulations, or procedures necessary to exercise the authority provided by this [chapter] *subchapter.*

§ 3517. Consultation with other agencies and the public

(a) In developing information resources management policies, plans, rules, regulations, procedures, and guidelines and in reviewing collections of information, the Director shall provide interested agencies and persons early and meaningful opportunity to comment.

(b) Any person may request the Director to review any collection of information conducted by or for an agency to determine, if, under this [chapter] *subchapter,* a person shall maintain, provide, or disclose the information to or for the agency. Unless the request is frivolous, the Director shall, in coordination with the agency responsible for the collection of information—

(1) respond to the request within 60 days after receiving the request, unless such period is extended by the Director to a specified date and the person making the request is given notice of such extension; and

(2) take appropriate remedial action, if necessary.

§ 3518. Effect on existing laws and regulations

(a) Except as otherwise provided in this [chapter] *subchapter,* the authority of an agency under any other law to prescribe policies, rules, regulations, and procedures for Federal information resources management activities is subject to the authority of the Director under this [chapter] *subchapter.*

(b) Nothing in this [chapter] *subchapter* shall be deemed to affect or reduce the authority of the Secretary of Commerce or the Director of the Office of Management and Budget pursuant to Reorganization Plan No. 1 of 1977 (as amended) and Executive order, relating to telecommunications and information policy, procurement and management of telecommunications and information systems, spectrum use, and related matters.

(c)(1) Except as provided in paragraph (2), this [chapter] *subchapter* shall not apply to the collection of information—

(A) during the conduct of a Federal criminal investigation or prosecution, or during the disposition of a particular criminal matter;

(B) during the conduct of—

(i) a civil action to which the United States or any official or agency thereof is a party; or

(ii) an administrative action or investigation involving an agency against specific individuals or entities;

(C) by compulsory process pursuant to the Antitrust Civil Process Act and section 13 of the Federal Trade Commission Improvements Act of 1980; or

(D) during the conduct of intelligence activities as defined in section 3.4(e) of Executive Order No. 12333, issued December 4, 1981, or successor orders, or during the conduct of cryptologic activities that are communications security activities.

(2) This [chapter] *subchapter* applies to the collection of information during the conduct of general investigations (other than information collected in an antitrust investigation to the extent provided in subparagraph (C) of paragraph (1)) undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.

(d) Nothing in this [chapter] *subchapter* shall be interpreted as increasing or decreasing the authority conferred by Public Law 89–306 on the Administrator of the General Services Administration, the Secretary of Commerce, or the Director of the Office of Management and Budget.

(e) Nothing in this [chapter] *subchapter* shall be interpreted as increasing or decreasing the authority of the President, the Office of Management and Budget or the Director thereof, under the laws of the United States, with respect to the substantive policies and programs of departments, agencies and offices, including the substantive authority of any Federal agency to enforce the civil rights laws.

* * * * * * *

§ 3520. Authorization of appropriations

There are authorized to be appropriated to the Office of Information and Regulatory Affairs to carry out the provisions of this [chapter] *subchapter,* and for no other purpose, $8,000,000 for each of the fiscal years 1996, 1997, 1998, 1999, 2000, and 2001.

Subchapter II—Information Security

§ 3531. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets;

(2)(A) recognize the highly networked nature of the Federal computing environment including the need for Federal Government interoperability and, in the implementation of improved security management measures, assure that opportunities for interoperability are not adversely affected; and

(B) provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems; and

(4) provide a mechanism for improved oversight of Federal agency information security programs.

§ 3532. Definitions

(a) Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) As used in this subchapter the term—

(1) "information technology" has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

(2) "mission critical system" means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that—

(A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);

(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; or

(C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

§ 3533. Authority and functions of the Director

(a)(1) The Director shall establish governmentwide policies for the management of programs that—

(A) support the cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations; and

(B) include information technology architectures as defined under section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425).

(2) Policies under this subsection shall—

(A) be founded on a continuing risk management cycle that recognizes the need to—

(i) identify, assess, and understand risk; and

(ii) determine security needs commensurate with the level of risk;

(B) implement controls that adequately address the risk;

(C) promote continuing awareness of information security risk; and

(D) continually monitor and evaluate policy and control effectiveness of information security practices.

(b) The authority under subsection (a) includes the authority to—

(1) oversee and develop policies, principles, standards, and guidelines for the handling of Federal information and information resources to improve the efficiency and effectiveness of governmental operations, including principles, policies, and guidelines for the implementation of agency responsibilities under applicable law for ensuring the privacy, confidentiality, and security of Federal information;

(2) consistent with the standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729), require Federal agencies to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency;

(3) direct the heads of agencies to

(A) identify, use, and share best security practices;

(B) develop an agency-wide information security plan;

(C) incorporate information security principles and practices throughout the life cycles of the agency's information systems; and

(D) ensure that the agency's information security plan is practiced throughout all life cycles of the agency's information systems;

(4) oversee the development and implementation of standards and guidelines relating to security controls for Federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

(5) oversee and coordinate compliance with this section in a manner consistent with—

(A) sections 552 and 552a of title 5;

(B) sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 and 278g–4);

(C) section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

(D) sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729); and

(E) related information management laws; and

(6) take any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) that the Director considers appropriate, including any action involving the budgetary process or appropriations management process, to enforce accountability of the head of an agency for information resources management, including the requirements of this subchapter, and for the investments made by the agency in information technology, including—

(A) recommending a reduction or an increase in any amount for information resources that the head of the agency proposes for the budget submitted to Congress under section 1105(a) of title 31;

(B) reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources; and

(C) using other authorized administrative controls over appropriations to restrict the availability of funds for information resources.

(c) The authorities of the Director under this section may be delegated—

(1) to the Secretary of Defense and the Director of Central Intelligence in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2); and

(2) in the case of all other Federal information systems, only to the Deputy Director for Management of the Office of Management and Budget.

§3534. Federal agency responsibilities

(a) The head of each agency shall—

(1) be responsible for—

(A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets;

(B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and

(C) ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system;

(2) ensure that appropriate senior agency officials are responsible for—

(A) assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control;

(B) determining the levels of information security appropriate to protect such operations and assets; and

(C) periodically testing and evaluating information security controls and techniques;

(3) delegate to the agency Chief Information Officer established under section 3506, or a comparable official in an agency

not covered by such section, the authority to administer all functions under this subchapter including—

(A) designating a senior agency information security official who shall report to the Chief Information Officer or a comparable official;

(B) developing and maintaining an agencywide information security program as required under subsection (b);

(C) ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(5) ensure that the agency Chief Information Officer, in coordination with senior agency officials, periodically—

(A)(i) evaluates the effectiveness of the agency information security program, including testing control techniques; and

(ii) implements appropriate remedial actions based on that evaluation; and

(B) reports to the agency head on—

(i) the results of such tests and evaluations; and

(ii) the progress of remedial actions.

(b)(1) Each agency shall develop and implement an agencywide information security program to provide information security for the operations and assets of the agency, including operations and assets provided or managed by another agency.

(2) Each program under this subsection shall include—

(A) periodic risk assessments that consider internal and external threats to—

(i) the integrity, confidentiality, and availability of systems; and

(ii) data supporting critical operations and assets;

(B) policies and procedures that—

(i) are based on the risk assessments required under subparagraph (A) that cost-effectively reduce information security risks to an acceptable level; and

(ii) ensure compliance with—

(I) the requirements of this subchapter;

(II) policies and procedures as may be prescribed by the Director; and

(III) any other applicable requirements;

(C) security awareness training to inform personnel of—

(i) information security risks associated with the activities of personnel; and

(ii) responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks;

(D)(i) periodic management testing and evaluation of the effectiveness of information security policies and procedures; and

(ii) a process for ensuring remedial action to address any significant deficiencies; and

(E) procedures for detecting, reporting, and responding to security incidents, including—

(i) mitigating risks associated with such incidents before substantial damage occurs;

(ii) notifying and consulting with law enforcement officials and other offices and authorities;

(iii) notifying and consulting with an office designated by the Administrator of General Services within the General Services Administration; and

(iv) notifying and consulting with an office designated by the Secretary of Defense and the Director of Central Intelligence for incidents involving systems described under subparagraphs (A) and (B) of section 3532(b)(2).

(3) Each program under this subsection is subject to the approval of the Director and is required to be reviewed at least annually by agency program officials in consultation with the Chief Information Officer. In the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), the Director shall delegate approval authority under this paragraph to the Secretary of Defense and the Director of Central Intelligence.

(c)(1) Each agency shall examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

(A) annual agency budgets;

(B) information resources management under the Paperwork Reduction Act of 1995 (44 U.S.C. 101 note);

(C) performance and results based management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 through 2805 of title 39; and

(E) financial management under—

(i) chapter 9 of title 31, United States Code, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

(ii) the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note) (and the amendments made by that Act); and

(iii) the internal controls conducted under section 3512 of title 31.

(2) Any significant deficiency in a policy, procedure, or practice identified under paragraph (1) shall be reported as a material weakness in reporting required under the applicable provision of law under paragraph (1).

(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Chief Information Officer, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods; and

(B) the resources, including budget, staffing, and training,

which are necessary to implement the program required under subsection (b)(1).

(2) The description under paragraph (1) shall be based on the risk assessment required under subsection (b)(2)(A).

§3535. Annual independent evaluation

(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency.

(2) Each evaluation under this section shall include—

(A) an assessment of compliance with—

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines; and

(B) tests of the effectiveness of information security control techniques.

(3) The Inspector General or the independent evaluator performing an evaluation under this section including the Comptroller General may use any audit, evaluation, or report relating to programs or practices of the applicable agency.

(b)(1)(A) Subject to subparagraph (B), for agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required under this section or, in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), an audit of the annual evaluation required under this section, shall be performed by the Inspector General or by an independent evaluator, as determined by the Inspector General of the agency.

(B) For systems described under subparagraphs (A) and (B) of section 3532(b)(2), the evaluation required under this section shall be performed only by an entity designated by the Secretary of Defense of the Director of Central Intelligence as appropriate.

(2) For any agency to which paragraph (1) does not apply, the head of the agency shall contract with an independent evaluator to perform the evaluation.

(3) An evaluation of agency information security programs and practices performed by the Comptroller General may be in lieu of the evaluation required under this section.

(c) Not later than 1 year after the date of enactment of this subchapter, and on that date every year thereafter, the applicable agency head shall submit to the Director—

(1) the results of each evaluation required under this section, other than an evaluation of a system described under subparagraph (A) or (B) of section 3532(b)(2); and

(2) the results of each audit of an evaluation required under this section of a system described under subparagraph (A) or (B) of section 3532(b)(2).

(d) Each year the Comptroller General shall—

(1) review the evaluations required under this section and other information security evaluation results; and

(2) report to Congress regarding the adequacy of agency information programs and practices.

(e) Agencies and evaluators shall take appropriate actions to ensure the protection of information, the disclosure of which may ad-

versely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws.

○

Document No. 30