Union Calendar No. 479

107TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
107–764

MAKING FEDERAL COMPUTERS SECURE: OVERSEEING EFFECTIVE INFORMATION SECURITY MANAGEMENT

THIRD REPORT

BY THE

COMMITTEE ON GOVERNMENT REFORM

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

OCTOBER 24, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

82–177 PDF WASHINGTON : 2002

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
Washington, DC, October 24, 2002.

Hon. J. DENNIS HASTERT,
Speaker of the House of Representatives,
Washington, DC.

DEAR MR. SPEAKER: By direction of the Committee on Government Reform, I submit herewith the committee's third report to the 107th Congress. The committee's report is based on a study conducted by its Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.

DAN BURTON,
Chairman.

CONTENTS

APPENDIXES

Union Calendar No. 479

107TH CONGRESS, *2d Session* | HOUSE OF REPRESENTATIVES | REPORT 107–764

MAKING FEDERAL COMPUTERS SECURE: OVERSEEING EFFECTIVE INFORMATION SECURITY MANAGEMENT

OCTOBER 24, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BURTON, from the Committee on Government Reform submitted the following

THIRD REPORT

On October 9, 2002, the Committee on Government Reform approved and adopted a report entitled "Making Federal Computers Secure: Overseeing Effective Information Security Management." The chairman was directed to transmit a copy to the Speaker of the House.

I. SUMMARY OF OVERSIGHT FINDINGS AND RECOMMENDATIONS

A. INTRODUCTION

The Committee on Government Reform (the "committee") has legislative jurisdiction with respect to the "overall economy, efficiency, and management of government operations and activities."[1] The committee also has the general oversight responsibility:

> [T]o determine whether laws and programs addressing subjects within the jurisdiction of [the] committee are being implemented and carried out in accordance with the intent of Congress and whether they should be continued, curtailed, or eliminated. Each standing committee (other than the Committee on Appropriations) shall review and study on a continuing basis the application, administration, execution, and effectiveness of laws and programs addressing subjects within its jurisdiction. [The committee shall review and study] any condition or circumstances that may indicate the necessity or desirability of enacting

[1] Clause 1(h)(6) rule X of the Rules of the House of Representatives, 107th Congress.

new or additional legislation addressing subjects within its jurisdiction.[2] Moreover, the committee has the special oversight function to "review and study on a continuing basis the operation of Government activities at all levels with a view to determining their economy and efficiency."[3]

The Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations (the "subcommittee") has legislative jurisdiction with respect to all matters relating to the handling of Government information, including information security.

Pursuant to this authority, the subcommittee convened five oversight hearings to explore:

- the extent of potential threats to Government operations posed by computer viruses and worms;
- the likelihood of cyber attacks against the Nation's information infrastructure;
- the status of efforts at major executive branch departments and agencies ("the agencies") to strengthen the security of their critical computer operations and assets;
- lessons learned from the Government Information Security Reform Act of 2000; and
- the need to reauthorize and strengthen the Government Information Security Reform Act.

Federal agencies rely extensively on computerized systems and electronic data to support operations that are essential to the health and well being of all Americans. Critical Government systems, from national defense and emergency services to tax collection and benefit payments, rely on electronically stored information and automated systems. Maintaining adequate security over these systems and the electronic data stored in them is essential to maintaining the continuity of the Government's critical operations. Security measures must prevent data tampering, fraud, sabotage and the inappropriate disclosure of sensitive information. Nevertheless, independent audits and evaluations continue to show that most Federal departments and agencies have pervasive weaknesses in their computer security programs that pose serious risks to these critical automated systems.

Federal computers have been successfully attacked at the Executive Office of the President, the Department of Defense, the Department of the Treasury and the Department of the Interior. The number and sophistication of these attacks are increasing, not only in the Federal Government but in private industry as well. In 2001, worms and viruses[4] such as Code Red, Code Red II, SirCam and Nimda affected millions of public and private computer users, shutting down Web sites, slowing Internet service and disrupting some Government operations. Overall, they have caused billions of

---

[2] Ibid., Clause 2(b)(1) (A) and (C).

[3] Ibid., Clause 3(e).

[4] A virus is a program that self-replicates, infecting files by inserting or attaching a copy of itself or by rewriting files. A worm is a program that propagates itself through networks, without any user intervention or interaction, by attacking other machines and copying itself to them. Worms often go undetected until their uncontrolled replication consumes system resources, slowing or halting other tasks. As viruses and worms advance, the difference between the two becomes negligible, and it is common to find malicious software that includes the characteristics of both of these once relatively distinct species.

dollars in damage. The September 11, 2001, terrorist attacks on the Nation's physical structure also raised the likelihood that terrorists might launch disruptive attacks against the Nation's information infrastructure.

The Government Information Security Reform Act of 2000 (Security Act)[5] was enacted during the 106th Congress to provide a comprehensive framework for ensuring that Federal departments and agencies implement effective security controls over information resources that support Federal operations and assets. The Security Act requires the agencies to implement agencywide information security programs that are founded on a continuing risk-management cycle. These programs, which are to be overseen by agencies' Chief Information Officers, are to be reviewed annually by program officials. In addition, the Security Act requires annual, independent evaluations of the agencies' computer security programs and practices, including control testing and compliance assessment.

The Office of Management and Budget [OMB] is responsible for overseeing Federal information security. The OMB guidance implementing the Security Act requires agencies to submit the results of their annual program reviews in an executive summary consisting of two components. The first component, which is prepared by agency Inspectors General, characterizes the results of their independent evaluations. The second component, which is prepared by agency Chief Information Officers, summarizes the results of the annual program reviews by agency officials. These reports and summaries served as the basis for the OMB's February 2002 report, "FY 2001 Report to Congress on Federal Government Information Security Reform." The OMB report identified six governmentwide security weaknesses that require correction, including the need to:

- greatly increase the degree of senior management attention to security;
- establish measures of performance to ensure that senior agency management can evaluate the performance of officials with security responsibilities;
- improve security education and awareness;
- fully integrate security into the capital planning and investment control process;
- ensure that contractor services are adequately secure; and
- improve agencies' ability to detect, report and share information on vulnerabilities.

B. FINDINGS

Based on oversight hearings conducted by the subcommittee, General Accounting Office [GAO] audits, Inspector General evaluations, the OMB report and the President's fiscal year 2003 budget submission, the committee finds that, although agencies are making progress in reducing information technology risks, the Federal Government continues to face formidable challenges in protecting its information system assets and sensitive data. Specifically, the committee finds that:

[5] Floyd D. Spence, National Defense Authorization Act for Fiscal Year 2001, P.L. 106–398, Title X, Subtitle G, 114 Stat. 1654, 1654A–265 (200).

1. Agencies are not conducting periodic risk assessments.

The Security Act requires agencies to perform periodic threat-based risk assessments of their systems and data. Although many agencies are making progress in addressing information security controls, most agencies have neither systematically identified their critical systems nor assessed the risks to those systems. In order to complete a systematic risk assessment, agencies must:

- inventory all resources under their control and systematically prioritize those resources based on their impact to the agency's mission; and
- identify and quantify the risks to systems and enterprises throughout the agency.

Without conducting systematic risk assessments, agencies have, by default, accepted an unknown level of risk. Although agencies may have some security controls and policies in place, without a risk assessment, they cannot know whether those security controls are appropriate for the level of risk to the system. Nor can agencies determine whether their planned remedial actions adequately address crucial hidden security weaknesses.

2. Federal computer systems have significant and pervasive weaknesses in security controls.

The GAO and agency Inspectors General identified significant weaknesses in the policies, procedures and technical controls at all 24 major Federal departments and agencies included in the Chief Financial Officers Act of 1990 (the "CFO Act"). Security weaknesses were found in the following areas:

- management controls that provide the framework for ensuring that security risks are understood, and that effective controls are selected and properly implemented;
- access controls that limit or detect inappropriate access to computer resources to ensure that only authorized users can read, modify or delete data;
- software development and change controls to ensure that only authorized software programs and modifications are implemented;
- controls that ensure an appropriate segregation of duties to reduce the risk that any one person could perform inappropriate actions without detection;
- operating system software controls to protect sensitive programs that support multiple applications; and
- service continuity controls to ensure that computer-dependent operations experience no significant disruption.

Significant weaknesses in security controls are so pervasive that in fiscal year 2001, GAO auditors found that 15 of the 24 major Federal agencies had weaknesses in all of the six control categories. All 24 agencies had weaknesses in their systems' program management and access controls. Those control weaknesses extended to critical Government operations, including e-government and e-commerce programs. For example, some of the General Service Administration's e-commerce and e-government systems such as GSA Advantage, FedPay, FedBiz Ops, ITSS and TOPS lack program management controls, including current risk assessments, certification/accreditation, security plans and system testing.

a. Agencies do not have effective security management program controls.

The Security Act requires agencies to implement agencywide information security programs that are founded on a continuing risk-management cycle. Agency program officials, Inspectors General, the GAO and the OMB all reported that agencies had not complied with this requirement. Specifically, most agencies had not developed security plans for major systems based on assessed risks; had not formally documented security policies and procedures; had not provided adequate computer security training to their employees; and did not have adequate procedures for detecting, reporting and responding to security incidents. In addition, most agencies had not implemented programs for testing and evaluating the effectiveness of the controls they rely on.

Although many agencies had remedial efforts underway to address the significant systems vulnerabilities identified by auditors, those efforts will not be fully effective or lasting until they are supported by the framework of a strong, agencywide security management program.

b. Agencies do not have effective access controls.

Agencies lack effective access controls' including site access controls, password controls, user and administrative permissions and network perimeter controls such as firewalls. The lack of these access controls allows intruders to modify, destroy or disclose sensitive information. In today's highly interconnected computing environment, weak access controls expose an agency's information and operations to attacks from remote locations by individuals with only minimal computer resources and skills.

3. Federal information technology systems rely on commercial software that is vulnerable to attack.

Commercial off-the-shelf operating systems and applications software have become increasingly complex. A single operating system or applications program may contain more than a billion lines of code. The size and complexity of the code makes detection of design and coding flaws difficult—especially if the flaws do not affect the operational functionality of the software being tested. Further, commercial software is inherently designed to facilitate the conduct of business through collaboration and information sharing, which, by its nature, is susceptible to being accessed by unauthorized individuals. In addition, to retain a competitive edge in the marketplace, software developers have focused on increasing software functionality and then speeding those features to market. This emphasis frequently comes at the expense of identifying potential software security flaws during the design and testing of new products. Some of those design and coding flaws leave the system vulnerable to attack.

According to the CERT® Coordination Center, 7,181 software vulnerabilities have been reported since 1995. The most common operating systems used by Federal agencies contain a substantial number of those vulnerabilities. In the past 5 years, 235 security vulnerabilities have been found in the Microsoft Windows NT operating system, 104 vulnerabilities in Microsoft 95/98, and 146

vulnerabilities in Solaris.[6] Correcting these vulnerabilities requires downloading software patches developed by the manufacturer. To be effective, these patches must be current, correctly installed and applied to all computers on a network. The number of new vulnerabilities being discovered daily makes remediating them an overwhelming task for systems administrators. This task is further complicated when the software patches to correct these vulnerabilities have other unintended consequences that must be corrected as well.

The complexity of commercial software is perhaps the most significant factor in creating vulnerabilities, but it is not the only factor. Commercial network configurations themselves are complex and unique to each user's data processing and storage requirements. The correct security settings depend on the specific network configuration and operating environment. For example, correct security settings depend on the type of routers, firewall and intrusion detection software, operating environment, and applications software and hardware. Until recently, commercial vendors shipped software with the default "out of the box" security settings disabled. Although that practice changed in 2001, most software is still shipped with security settings only partially enabled because the optimal settings depend on the specific network configuration. Systems administrators must set a multitude of security parameters in an increasingly complex and unique network environment—security parameters that must be re-assessed each time an organization's mission changes, or when software or hardware is modified.

The Government's reliance on commercial software exposes Federal agencies to the same types of cyber attacks faced by the private sector. Exploit scripts,[7] which hackers use to attack these vulnerabilities, are traded in an underground forum. Government systems make unusually attractive targets because of the critical information they store.

4. Agencies' Capital Planning and Investment Control processes do not include information technology security.

Implementation of a robust Capital Planning and Investment Control [CPIC] process for information technology would provide agencies with an institutionalized, formal process for planning and evaluating their information technology investments. The CPIC process must include security requirements and costs as part of planning and investment decisionmaking if agencies are to make informed risk/benefit investment decisions. Even those agencies that have implemented a robust CPIC process do not, in all cases, include security considerations in their formal processes. Only two of the agencies reviewed (the Departments of Agriculture and Labor) had a strong, implemented CPIC process that included security requirements.

Unless computer security is fully integrated into an institutionalized CPIC process, the Government is at risk of continuing to in-

[6] Security Focus Online, http://online.securityfocus.com/vulns/stats/shtml, Feb. 27, 2002.

[7] Exploit scripts are software programs used by hackers to take advantage of system vulnerabilities in order to take control of the victim's computer system and execute malicious actions.

vest billions of dollars in unsecured information technology systems.

5. Congress does not have consistent and timely access to the information it needs to fulfill its oversight responsibilities for Federal information security and related budget deliberations.

Under the reporting requirements of the Security Act, agencies are required to report the results of their independent evaluations to the OMB. The OMB requires agencies to submit plans that identify, assess, prioritize and monitor the progress of their efforts to correct identified security weaknesses. Together, these evaluations and plans provide essential information regarding agencies' identified vulnerabilities, and their progress and commitment toward rectifying those vulnerabilities. Although the OMB provides Congress with an annual summary of these evaluations, Congress does not have consistent and timely access to the level of information it requires to monitor the status of agency computer security efforts.

During the 107th Congress, the subcommittee reviewed the President's Fiscal Year 2003 budget to assess whether agencies were making adequate investments to correct the security weaknesses identified in the OMB summary report to Congress. However, there was such a wide disparity in the level of information reported by agencies that no determination could be made. For example, the Departments of Energy, Justice, Labor and the Treasury specifically proposed budgets to correct most, if not all, of their identified material weaknesses. However, the remaining budget proposals did not include sufficient information to determine whether identified security weaknesses would be addressed or not. Specifically, neither the Department of the Interior nor the Department of Transportation reported on any projects relating to security enhancements. Last year, both departments received "F's" on the subcommittee's computer security report card.

To oversee the Government's computer security efforts, Congress must have access to a full range of information, including specific agency vulnerabilities and agency efforts to rectify those vulnerabilities, including plans, milestones, resources and status.

C. RECOMMENDATIONS

Based on the foregoing findings, the committee recommends the following:

1. The Government Information Security Reform Act of 2000 (Security Act) should be strengthened and made permanent.

The Security Act requires Federal agencies to implement agency-wide information security programs based on the level of risk to their systems, to provide annual independent evaluations of their information security programs, and to report the results of those evaluations to the OMB. The Security Act's requirements have provided Congress and the administration with a more complete and accurate picture of security weaknesses within Federal information systems. The requirements of the act have also established a benchmark with which to measure agency progress. However, the Security Act expires on November 29, 2002. Allowing this act to expire would undermine agencies' commitment toward enhancing

their information security programs. Moreover, it would eliminate a significant source of information for overseeing the effectiveness of agency computer security programs and measuring their progress. The act has been instrumental in attracting the attention of top agency management to the importance of computer security, and agencies are beginning to address their pervasive systems vulnerabilities. Congress needs to sustain this momentum and strengthen the Security Act by enacting H.R. 3844, the "Federal Information Security Management Act of 2002." The provisions of this legislation would:

- reauthorize and expand the Security Act's requirements for annual agency computer security evaluations and reporting;
- require the development, promulgation and compliance with minimum mandatory management controls for securing information and information systems;
- improve accountability and congressional oversight by clarifying the Security Act's reporting requirements and ensuring that Congress and the GAO have access to information security evaluation results;
- clarify the Security Act's requirements for national security systems;
- strengthen agency information security programs, update the responsibilities of the National Institute of Standards and Technology; and
- clarify definitions and legislative language.

2. Sustained congressional oversight is needed.

Strong, sustained congressional oversight is needed to ensure that Federal agencies implement adequate agencywide security programs. Thus, Congress should continue oversight reviews of agency efforts to comply with the requirements of the Security Act and any ensuing reform legislation. As well, detailed information on agency computer security efforts, which has been mandated by the OMB, should be made available to relevant congressional committees and the GAO.

3. Agency funding should be tied to the implementation of effective computer security plans and procedures.

If agencies fail to dedicate the appropriate resources toward resolving their information security problems, Congress should provide additional incentives. The OMB is appropriately using the budget process to ensure that computer security becomes a priority of agency management. Furthermore, the OMB has directed agencies to prepare and submit plans of action and milestones for all programs and systems in which a security weakness has been found. The OMB has stated that it will stop funding information technology projects that do not adequately address security requirements or requests that neglect to document how security planning and funding are integrated into the life cycle of the projects. It is too early to evaluate the success of this action, however. If substantial improvements to agency security policies, processes and practices are not made, Congress should consider using its authority to redirect a percentage of the agency's appropriated funds toward correcting significant security weaknesses.

4. Congress should encourage the administration to set minimum security standards for commercial off-the-shelf software that is purchased by Federal agencies.

To the extent practical, the Federal Government must become an informed consumer and avoid purchasing commercial software that contains long-standing and significant vulnerabilities. The current practice of releasing software without adequate security testing and then developing patches to fix vulnerabilities creates an untenable burden on Government systems administrators. Federal agencies need a list of qualified software products. The list could be based on specified tests conducted by the developer or an independent Government agency, such as the National Institute of Standards and Technology or the National Security Agency; adaptation of a software maturity model targeted specifically to security processes and practices; or a combination of tests and process certifications.

II. CONCLUSIONS

Poor computer security is a governmentwide problem. Although several agencies have recently taken noteworthy steps to strengthen their information security programs, subcommittee hearings and other reports continue to find significant security weaknesses in computer systems at all 24 major Federal departments and agencies. Such weaknesses leave the Government's critical operations and assets highly vulnerable to cyber attacks.

In November 2001, the subcommittee gave the Government an overall grade of "F" for its efforts to protect Federal computer systems. This failure should serve as an urgent warning that agencies are not making adequate progress in addressing their computer security vulnerabilities. The number and sophistication of attacks on Government computers continue to escalate, thus, increasing the risk to vulnerable Federal computer systems and networks.

Agencies must establish effective agencywide security-management programs that ensure that sensitive data and critical operations are protected. Each program should incorporate a strong set of management procedures and an organizational framework to identify and assess risks, decide what policies and controls are needed, periodically evaluate the effectiveness of policies and controls, and take action to address identified weaknesses.

The evaluation and reporting requirements of the Security Act provide a more complete evaluation of Federal information security efforts than was previously available. Accordingly, the reports will allow more effective oversight of agency efforts to identify and correct information system vulnerabilities.

Following the terrorist attacks on September 11, 2001, the President's Special Advisor for Cyberspace Security warned that the enemies of this Nation fully understand the United States' reliance on technology and are looking for vulnerabilities to exploit. It is imperative that Federal agencies work diligently to ensure that the computer systems that support their critical operations and the sensitive data they store are adequately protected.

III. SUBCOMMITTEE INITIATIVES

A. Oversight hearing on the extent of the potential threat posed by computer viruses and worms to the workings of the Federal Government.

The subcommittee held an oversight hearing on computer security in San Jose, CA, on August 29, 2001. The hearing focused on the threats posed by computer viruses and worms to Government operations. Witnesses from both Government and industry highlighted the damage caused by a recent rash of computer virus and worm attacks. They warned that these viruses and worms are becoming increasingly sophisticated and virulent. Those attacks could foreshadow potentially more damaging and devastating threats to the Nation's critical infrastructures. Accordingly, witnesses emphasized the need for proactive measures to protect critical operations and assets. As in previous reports and testimonies, the General Accounting Office noted the importance of Federal agencies establishing strong agencywide security management programs that include robust security planning, training and oversight. Witnesses from the National Security Agency and the Federal Bureau of Investigation emphasized the importance of better coordination among key Federal organizations to improve their detection, prevention and mitigation capabilities. Security experts from both the Government and the private sector also stressed the importance of designing more secure software products, the need for Federal support of research and development in computer security, and the need for university programs in information security. A witness from Symantec, one of the leading Internet security technology companies, stated that agencies could prevent 80 percent of possible attacks by adopting the top 20 percent of good security practices, several of which are as simple as using well-chosen passwords.

B. Oversight hearing on the probability of cyber attacks against the Nation's computer-dependent infrastructure.

Following the September 11, 2001, attacks on New York City and Washington, DC, the subcommittee held an oversight hearing on computer security on September 26, 2001. This hearing focused on the potential threat of cyber attacks by terrorists. In addition, the hearing examined the Nation's preparedness to deal with such attacks, and what actions must be taken to protect the Nation's vital information technology infrastructure. Based on recent precedents, cyber attack trends and the geopolitical situation, the Director of the Institute for Security Technology Studies at Dartmouth College stated that the probability of cyber attacks against the U.S. information infrastructure was quite high. Witnesses from the Government underscored that pervasive security weaknesses in Federal information systems make the risk of disruption to critical operations extremely likely. A witness from the New York Mercantile Exchange emphasized that the September 11 events created new and unprecedented security demands. These demands, such as the need for comprehensive contingency plans for restoring critical operations, apply to cyber defense as well as to the defense of the Nation's physical infrastructure.

C. Report card grading Federal departments and agencies on their computer security efforts.

On November 9, 2001, the subcommittee held another hearing on computer security, during which it released its second annual report card measuring the Federal Government's progress in securing its computer systems. The grades were primarily based on agency summary reports to the OMB. These reports were based on the results of agency program reviews and independent evaluations by agency Inspectors General and Chief Information Officers, as required by the Security Act. Hearing witnesses from both the GAO and the OMB emphasized the importance of annual evaluations and reports in holding agencies accountable for implementing effective security. They noted that these mechanisms enable Congress and the administration to monitor agency performance and to take whatever oversight action is deemed advisable to remedy identified problems.

The subcommittee's grades provided a high-level assessment of the agencies' overall computer security programs and implementation. Armed with more detailed information than in the previous year, the subcommittee determined that the Federal Government earned a failing grade of "F" for its computer security efforts. Two-thirds of the agencies evaluated, including such critical agencies as the Departments of Defense, Energy, Transportation, and Health and Human Services, as well as the Nuclear Regulatory Commission, failed completely in their computer security efforts. Five agencies received a barely passing grade of "D." They included the Federal Emergency Management Agency, the General Services Administration and the Department of State. The National Aeronautics and Space Administration and the Social Security Administration both scored "C's." The National Science Foundation earned the highest grade—a "B-plus."[8]

D. Oversight hearing on lessons learned from the Government Information Security Reform Act of 2000.

On March 6, 2002, the subcommittee held a hearing on computer security to assess the lessons learned from the Security Act. The hearing focused on implementation of the Security Act and, in particular, its effectiveness in improving the security of Federal information systems. During the hearing, the subcommittee examined the development and promulgation of security standards; the development of agency security programs; and the oversight roles of agency heads, the Director of the OMB and the GAO.

Witnesses from the GAO, the OMB and Federal agencies all emphasized the value of the act's reporting requirements in fostering senior management accountability and attention to computer security issues. As well, it established a security baseline from which to measure future agency progress in improving computer security. The GAO witness testified that agencies had made a significant first step in implementing the requirements of the act; however, they had not established information security programs consistent with the act's requirements. Significant weaknesses still existed in the areas of providing security policy guidance, conducting risk as-

[8] See Appendix A.

sessments, developing agencywide security programs, implementing adequate security controls, establishing security incident centers and conducting security training. The OMB witness emphasized that its oversight role, which focuses on management implementation of security, will be supported by the incorporation of security performance measurements in the President's Management Scorecard. Agency witnesses identified specific strategies their agencies were using to improve implementation of the act. These strategies included reforming accreditation and certification processes, improving information technology investment review processes and focusing security protections on their highest priority assets.

E. Legislative hearing on the "Federal Information Security Management Act of 2002."

On May 2, 2002, the subcommittee held a legislative hearing on H.R. 3844, the "Federal Information Security Management Act of 2002," introduced by Representative Tom Davis, R–VA. This bill would extend the essential provisions of the Government Information Security Reform Act of 2000 (Security Act), which will expire on November 29, 2002. H.R. 3844 would permanently authorize and strengthen the Government's information security program evaluation and reporting requirements. H.R. 3844 would also require the development, promulgation and agency compliance with minimum mandatory management controls for securing information and information systems. In addition, the bill would require annual agency reporting to the OMB, Congress and the Comptroller General, establish a Federal Information Security Incident Center, and clarify the definition of and evaluation responsibilities for national security systems.

Witnesses from the GAO, the OMB, agency Chief Information Officers and Inspectors General all emphasized the need to continue the security management and reporting requirements established in the Security Act. Although the Security Act has contributed to a substantially improved security posture, Federal information systems are far from secure. The GAO witness testified that continued authorization of Federal information security legislation is essential in order to sustain agency efforts toward implementing sound security practices, and identifying and correcting the significant weaknesses that exist in their systems.

APPENDIXES

APPENDIX A.—COMPUTER SECURITY REPORT CARD

Computer Security Report Card — November 9, 2001

Departments and Agencies	Grade	Departments and Agencies	Grade
NSF National Science Foundation	B+	**Education** Department of Education	F
		Energy Department of Energy	F
SSA Social Security Administration	C+	**HHS** Department of Health & Human Services	F
NASA National Aeronautics & Space Administration	C-	**Interior** Department of the Interior	F
EPA Environmental Protection Agency	D+	**Justice** Department of Justice	F
State Department of State	D+	**Labor** Department of Labor	F
FEMA Federal Emergency Management Agency	D	**NRC** Nuclear Regulatory Commission	F
GSA General Services Administration	D	**OPM** Office of Personnel Management	F
HUD Department of Housing and Urban Development	D	**SBA** Small Business Administration	F
Agriculture Department of Agriculture	F	**Transportation** Department of Transportation	F
AID Agency for International Development	F	**Treasury** Department of the Treasury	F
Commerce Department of Commerce	F	**VA** Department of Veterans Affairs	F
Defense Department of Defense	F	**Governmentwide Grade**	F

Prepared for Chairman Stephen Horn, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. Based on agency reports required by the Security Act of 2000, and GAO and Inspectors General audit reports issued from July 2000 through September 2001.

Subcommittee Home Page: http://www.house.gov/reform/gefmir.htm

APPENDIX B.—BASIS FOR AGENCY COMPUTER SECURITY GRADES

The subcommittee's computer security grades for each of the 24 major departments and agencies are based on information contained in agency reports to the Office of Management and Budget [OMB] and audit work conducted by agency Inspectors General and the General Accounting Office [GAO].

In June 2001, the OMB issued reporting guidance to agencies on implementing the Security Act.[9] This guidance outlined 10 specific topic areas that needed to be included in both the Chief Information Officers' and Inspectors General's executive summaries. These topic areas refer to the key elements of an effective computer-security program. In grading the agencies, the subcommittee assigned weighted point values to each of these topic areas, with a perfect score totaling 100 points.

As shown in the accompanying chart, "Analysis and Scoring Criteria," maximum point values were assigned to questions according to their importance to an agency's computer security program. Since most questions provide a range of possible responses, the number of points is proportional to the extent to which the element has been implemented. For example, agencies received zero (0) points for a response of "no," more points for "partially," and the full weighted value for "yes." Based on its analysis of the Chief Information Officers' and Inspector Generals' responses, the subcommittee tallied the scores for the 24 agencies.

Because the level of detail and/or responsiveness of reported data was uneven, the subcommittee also considered the results of computer security audits conducted by the General Accounting Office and agency Inspectors General from July 2000 through September 2001 examining security weaknesses:[10] Significant weaknesses have been identified for all agencies in some or all control categories. Those weaknesses indicate the extent to which agencies have actually implemented general controls.

Points were *subtracted* from the agency's score for each control area where significant weaknesses have been found. Conversely, if audit work did *not* identify significant weaknesses in a control area, a corresponding number of points were *added* to the agency's score. The point values total 20 points and are distributed as follows:

- Entity-wide security program planning and management—6 points;
- Access controls—5 points;
- Application development and change controls—2 points;
- System software controls—2 points;
- Segregation of duties controls—1 point; and
- Service continuity controls—4 points.

Finally, some agencies have one or more control areas that have not been sufficiently audited. Because it is unknown whether significant weaknesses exist in these areas, a number of points equal to half the assigned point value was *subtracted* from the agency's

[9] See Appendix C for OMB Reporting Guidelines.

[10] GAO routinely tracks the results of computer security audit work for the 24 major departments and agencies covered by the Chief Financial Officers Act. Results are shown in the accompanying chart entitled "Information Security Audit Results."

score. An exception was made in the "separation of duties" category, where the full value of 1 was subtracted in order to prevent using fractions. The final numerical score is the result of these adjustments.

Letter grades for the 24 agencies were assigned as follows:

90 to 100 = A
80 to 89 = B
70 to 79 = C
60 to 69 = D
59 and lower = F

The Government-wide grade was determined by averaging the final scores of all 24 agencies.

APPENDIX C.—ANALYSIS AND SCORING CRITERIA

Analysis and Scoring Criteria

Part I—Report Grading Element	Weight (100 Points Max)
1. Does the report identify the agency's total FY02 security funding budget request broken down by operating unit and critical infrastructure protection costs? (OMB Memorandum 00-07, Memorandum 97-02, and Circular A-11)	**5 points max**
Agency provided total FY02 budget request broken down by operating unit and critical infrastructure protection costs.	(5)
Agency provided total, but not broken down by operating unit and critical infrastructure protection costs.	(3)
No specific security funding information was provided.	(0)
2. Has the agency implemented an up-to-date information security methodology for identifying and prioritizing its critical assets, including links with key external systems? (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act)	**10 points max**
Methodology implemented, critical assets identified and ranked.	(10)
Methodology identified/developed but not fully implemented.	(5)
No.	(0)
3. Does the agency use measures of performance to ensure that program officials have: (1) assessed the risk to operations and assets under their control; (2) determined the level of security appropriate to protect such operations and assets; (3) maintained an up-to-date security plan that is practiced throughout the life cycle for each system supporting operations and assets under their control; and (4) tested and evaluated security controls? (Section 3534(a)(2) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established but not linked to any specific officials.	(8)
Performance measures are being developed, but were not implemented in 2001.	(8)
Performance measures not provided.	(0)
4. Does the agency use performance measures to ensure that the agency CIO adequately maintains an agency-wide security program, ensures the effective implementation of the program, and evaluates the performance of agency components? (Section 3534(a)(3)-(5) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established, but not specifically linked to the CIO.	(7)

Part I—Report Grading Element	Weight (100 Points Max)
Performance measures are being developed, but were not implemented in 2001.	(5)
Performance measures not provided.	(0)
5. Does the head of the agency use performance measures to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? (Section 3533(a)(1)(A)-(B), (b)(3)(C)-(D),(b)(6) and 3534(a)(C) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established but not specifically linked to the head of the agency.	(5)
Performance measures are being developed, but were not implemented in 2001.	(5)
Performance measures not provided.	(0)
6. Does the agency have mechanisms in place to ensure that contractor provided services or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy, and NIST guidance, national security policy, and agency policy? (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act)	**10 points max**
The agency does not have significant contractor provided services or services provided by another agency.	(10)
The agency has implemented mechanisms that provide independent assurance that 3rd party/contractor supported operations are adequately secure.	(10)
The agency has implemented mechanisms to ensure the security of 3rd party/contractor-supported operations but has taken no steps to verify that these are being implemented by the contractor.	(5)
The agency has not implemented mechanisms for gaining assurance that 3rd party/contractor-supported operations are adequately secure.	(0)
7. Are employees sufficiently trained in their security responsibilities? (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act) [Multiple responses—points awarded for each]	**15 points max**
Security awareness training provided in 2001.	(5)
Technical security-related training provided in 2001.	(5)
Total numbers of employees that received security training in 2001 provided.	(2.5)
Total cost for security training in 2001 provided.	(2.5)
8. Does the agency have documented procedures for reporting security incidents and sharing information? (Section 3534(b)(2)(F)(i)-(iii) of the Security Act)	**15 points max**

Part I—Report Grading Element	Weight (100 Points Max)
Procedures for reporting incidents and for sharing information have been fully developed and implemented.	(15)
Development of procedures for reporting incidents and for sharing information is in process or complete, but implementation is not complete.	(10)
9. Has the agency integrated security into its capital planning and investment control process? (Section 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act)	**10 points max**
Yes, the agency has integrated security into its capital planning and investment control process and reported security costs on every FY02 capital asset plan submitted to OMB.	(10)
Partially. The agency has generally integrated security into its capital planning process but has not begun reporting security costs on every capital asset plan.	(8)
No, the agency has not integrated security into capital planning.	(0)
10. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act)	**5 points max**
The agency has no PDD-63 identified CIP systems.	(5)
Yes.	(5)
No.	(0)

Part II—Adjustment for Security Weaknesses Identified in IG & GAO Audit Reports Issued From July 2000 through September 2001	Weight (20 Points Max)
General Control Categories:	
Entitywide program planning and management	(±6)
Access Controls	(±5)
Application Development and Change Controls	(±2)
Segregation of Duties	(±1)
System Software	(±2)
Service Continuity	(±4)

APPENDIX D.—INDEX OF WITNESSES

WILLEMSSEN, Joel, Managing Director, Information Technology Issues, U.S. General Accounting Office, September 26, 2001.

WILLIAMS, David C., Treasury Inspector General for Tax Administration, May 2, 2002.

WISER, Leslie G., Jr., section chief, National Infrastructure Protection Center, Federal Bureau of Investigation, August 29, 2001.

WOLF, Daniel G., Director, Information Assurance Directorate, National Security Agency, May 2, 2002.

WU, Benjamin H., Deputy Undersecretary of Commerce for Technology Administration, Department of Commerce, May 2, 2002.