United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations and the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Thursday,
May 2, 2002

INFORMATION SECURITY

Comments on the Proposed Federal Information Security Management Act of 2002

Statement of Robert F. Dacey
Director, Information Security Issues

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to discuss H.R. 3844, the Federal Information Security Management Act of 2002. This bill seeks to strengthen federal government information security by reauthorizing and expanding the information security, evaluation, and reporting requirements enacted into law as the Government Information Security Reform provisions (commonly referred to as "GISRA") in the National Defense Authorization Act for Fiscal Year 2001.[1] Concerned with reports that continuing, pervasive information security weaknesses place federal operations at significant risk of disruption, tampering, fraud, and inappropriate disclosures of sensitive information, the Congress enacted GISRA to reduce these risks and provide more effective oversight of federal information security.

As I stated in my March 6, 2002, testimony before the Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee, first-year implementation of GISRA represented a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses.[2] However, first-year implementation indicated areas in which GISRA could be strengthened and clarified to further improve federal information security and congressional oversight. Furthermore, GISRA will expire on November 29, 2002, less than a year away.

In my testimony today, I will first discuss the need to continue authorization of government information security legislation in view of the major information security risks that are facing federal agencies. Next, I will discuss major changes proposed in H.R. 3844, such as requiring annual agency reporting to the Office of Management and Budget (OMB) and the comptroller general, and establishing mandatory minimum security controls. Finally, I will highlight other changes in H.R. 3844 intended to clarify and streamline GISRA provisions.

Messrs. Chairmen, this testimony is based on our analysis of the proposed language of H.R. 3844 that you introduced in the House of Representatives on March 5, 2002. It is also based on the results of our review of first-year

[1]Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, October 30, 2000.

[2]U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

GISRA implementation as presented in my March 2002 testimony and in our report, which is being released today entitled, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*.[3] We performed our work during March and April 2002 in accordance with generally accepted government auditing standards.

Results In Brief

H.R. 3844 would permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA, which is to expire on November 29, 2002. As demonstrated by first-year implementation, GISRA proved to be a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. Agencies have noted benefits from GISRA, such as increased management attention to and accountability for information security. In addition, the administration has taken important actions to address information security, such as plans to integrate information security into the President's Management Agenda Scorecard. We believe that continued authorization of such important information security legislation is essential to sustaining agency efforts to identify and correct significant weaknesses. Further, this authorization would reinforce the federal government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

H.R. 3844 also proposes a number of changes and clarifications to strengthen information security, some of which address issues noted in the first-year implementation of GISRA. In particular, the bill requires the development, promulgation, and compliance with minimum mandatory management controls for securing information and information systems; creates a requirement for annual agency reporting to both OMB and the comptroller general; and clarifies the definition of and evaluation responsibilities for national security systems. In addition, the bill proposes other changes that would require federal agencies to strengthen their information security programs, update the information security responsibilities of the National Institute of Standards and Technology (NIST), and clarify or otherwise streamline definitions and legislative language.

[3]GAO-02-407, Washington, D.C.: May 2, 2002.

In addition to reauthorizing information security legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. However, this widespread interconnectivity also poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support, such as telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services. Likewise, the speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. Further, the events of September 11, 2001, underscored the need to protect America's cyberspace against potentially disastrous cyber attacks—attacks that could also be coordinated to coincide with physical terrorist attacks to maximize the impact of both.

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[4] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were

[4]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*. GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[5] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[6]

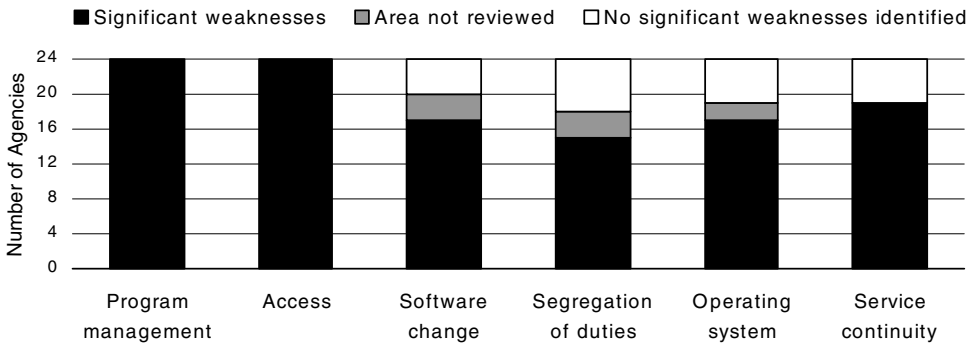
These weaknesses continue as indicated by our most recent analyses for these 24 large federal agencies that considered the results of inspector general (IG) and GAO audit reports published from July 2000 through September 2001, including the results of the IGs' independent evaluations of these agencies' information security programs performed as required by GISRA.[7] These analyses showed significant information security weaknesses in all major areas of the agencies' general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Figure 1 illustrates the distribution of weaknesses across the 24 agencies for the following six general control areas: (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

[5]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000).

[6]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update*, GAO/HR-99-1 (Washington, D.C.: Jan. 1999); *High Risk Series: An Update,* GAO-01-263 (Washington, D.C.: Jan. 2001).

[7]U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001).

Figure 1: Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued July 2000 through September 2001.

Our analyses showed that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 agencies (88 percent) in a similar analysis in 2000.[8] For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, the Congress enacted GISRA, which became effective November 29, 2000, and is in effect for 2 years after this date. GISRA supplements information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by OMB[9] and NIST,[10] as well as audit and best practice guidance issued by

[8]U.S. General Accounting Office, *Computer Security: Critical Federal Operations and Assets Remain at Risk*, GAO/T-AIMD-00-314 (Washington, D.C.: Sept. 11, 2000).

[9]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

[10]Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.

GAO.[11] Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establishes new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

The law assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and the IGs. OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. This includes the authority to approve agency information security programs, but delegates OMB's responsibilities regarding national security systems to national security agencies. OMB is also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. GISRA does not specify a date for this report.

Each agency, including national security agencies, is to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program is to include

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;
- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting and responding to security incidents; and
- an annual program review by agency program officials.

[11]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999); *Information Security Management: Learning from Leading* Organizations, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

In addition to the responsibilities listed above, GISRA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non–national-security systems are to be performed by the agency IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. For the evaluation of national security systems, special provisions include designation of evaluators by national security agencies, restricted reporting of evaluation results, and an audit of the independent evaluation performed by the IG or an independent evaluator. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

Finally, GISRA also assigns additional responsibilities for information security policies, standards, guidance, training, and other functions to other agencies. These agencies are NIST, the Department of Defense, the intelligence community, the Attorney General (Department of Justice), the General Services Administration, and the Office of Personnel Management.

H.R. 3844 Would Continue Benefits of Information Security Reform

With GISRA expiring on November 29, 2002, H.R. 3844 proposes to permanently authorize information security legislation that essentially retains the same purposes as GISRA, as well as many of GISRA's information security program, evaluation, and reporting requirements. It would also authorize funding to carry out its provisions for 5 years, thereby providing for periodic congressional oversight of the implementation and effectiveness of these requirements.

We believe that continued authorization of information security legislation is essential to improving federal information security. As emphasized in our March 2002 testimony, the initial implementation of GISRA was a significant step for agencies, the administration, and the Congress in addressing the serious, pervasive weaknesses in the federal government's information security.[12] GISRA consolidated security requirements that existed in law and policy before GISRA and put into law the following important additional requirements, which are continued in H.R. 3844.

First, GISRA requires agency program managers and CIOs to implement a risk-based security management program covering all operations and assets of the agency, including those provided or managed for the agency by others. Instituting such an approach is important since many agencies had not effectively evaluated their information security risks and

[12]GAO-02-470T, March 6, 2002.

implemented appropriate controls. Our studies of public and private best practices have shown that effective security program management requires implementing a process that provides for a cycle of risk management activities as now included in GISRA.[13] Moreover, other efforts to improve agency information security will not be fully effective and lasting unless they are supported by a strong agencywide security management program.

Second, GISRA requires an annual independent evaluation of each agency's information security program. Individually, as well as collectively, these evaluations can provide much needed information for improved oversight by OMB and the Congress. Our years of auditing agency security programs have shown that independent tests and evaluations are essential to verifying the effectiveness of computer-based controls. Audits can also evaluate an agency's implementation of management initiatives, thus promoting management accountability. Annual independent evaluations of agency information security programs will help drive reform because they will spotlight both the obstacles and progress toward improving information security and provide a means of measuring progress, much like the financial statement audits required by the Government Management Reform Act of 1994. Further, independent reviews proved to be an important mechanism for monitoring progress and uncovering problems that needed attention in the federal government's efforts to meet the Year 2000 computing challenge.[14]

Third, GISRA takes a governmentwide approach to information security by accommodating a wide range of information security needs and applying requirements to all agencies, including those engaged in national security. This is important because the information security needs of civilian agency operations and those of national security operations have converged in recent years. In the past, when sensitive information was more likely to be maintained on paper or in stand-alone computers, the main concern was data confidentiality, especially as it pertained to classified national security data. Now, virtually all agencies rely on interconnected computers to maintain information and carry out operations that are essential to their missions. While the confidentiality

[13]General Accounting Office, GAO/AIMD-98-68, Washington, D.C.: May 1998; *Information Security Risk Management: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: November 1999).

[14]U.S. General Accounting Office, *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges*, GAO/AIMD-00-290 (Washington, D.C.: Sept. 12, 2000).

needs of these data vary, all agencies must be concerned about the integrity and the availability of their systems and data. It is important for all agencies to understand these various types of risks and take appropriate steps to manage them.

Fourth, the annual reporting requirements provide a means for both OMB and the Congress to oversee the effectiveness of agency and governmentwide information security, measure progress in improving information security, and consider information security in budget deliberations. In addition to management reviews, annual IG reporting of the independent evaluation results to OMB and OMB's reporting of these results to the Congress provide an assessment of agencies' information security programs on which to base oversight and budgeting activities. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the OMB and congressional efforts to oversee the Year 2000 computer challenge. This reporting also facilitates a process to help ensure consistent identification of information security weaknesses by both the IG and agency management.

The first-year implementation of GISRA also yielded significant benefits in terms of agency focus on information security. A number of agencies stated that as a result of implementing GISRA, they are taking significant steps to improve their information security programs. For example, one agency stated that the law provided it with the opportunity to identify some systemic program-level weaknesses for which it plans to undertake separate initiatives targeted specifically to improve the weaknesses. Other benefits agencies observed included (1) higher visibility of information security within the agencies, (2) increased awareness of information security requirements among department personnel, (3) recognition that program managers are to be held accountable for the information security of their operations, (4) greater agency consideration of security throughout the system life cycle, and (5) justification for additional resources and funding needed to improve security. Agency IGs also viewed GISRA as a positive step toward improving information security particularly by increasing agency management's focus on this issue.

Implementation of GISRA has also resulted in important actions by the administration which, if properly carried out, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment, and NIST has established a Computer Security Expert Assist

Team to review agencies' computer security management. The administration also has plans to

- direct large agencies to undertake a review to identify and prioritize critical assets within the agencies and to identify their interrelationships with other agencies and the private sector;
- conduct a cross-government review to ensure that all critical government processes and assets have been identified;
- integrate security into the President's Management Agenda Scorecard;
- develop workable measures of performance;
- develop electronic training on mandatory topics, including security; and
- explore methods to disseminate vulnerability patches to agencies more effectively.

Such benefits and planned actions demonstrate the importance of GISRA's requirements and the significant impact they have had on information security in the federal government.

Major Changes Proposed by H.R. 3844

H.R. 3844 proposes a number of changes and clarifications that we believe could strengthen information security requirements, some of which address issues noted in the first-year implementation of GISRA.

Establishing Mandatory Minimum Controls

Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, some discretion is appropriate since, as OMB and NIST guidance state, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[15] In particular, specific mandatory standards for specified risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately and consistently protected; and reduce demands for already limited agency information security resources to independently develop security controls.

[15] GAO/AIMD-98-68, May 1998.

In response to this need, H.R. 3844 includes a number of provisions that would require the development, promulgation, and compliance with minimum mandatory management controls for securing information and information systems to manage risks as determined by agencies. Specifically,

- NIST, in coordination with OMB, would be required to develop (1) standards and guidelines for categorizing the criticality and sensitivity of agency information according to the control objectives of information integrity, confidentiality, and availability, and a range of risk levels, and (2) minimum information security requirements for each information category.

- OMB would issue standards and guidelines based on the NIST-developed information and would require agencies to comply with them. This increases OMB's information security authority, given that the secretary of commerce is currently required by the Computer Security Act to issue such standards. These standards would include (1) minimum mandatory requirements and (2) standards otherwise considered necessary for information security.

- Agencies may use more stringent standards than provided by NIST, but H.R. 3844 would require building more stringent protections on top of minimum requirements depending on the nature of information security risks.

- Waiver of the standards is not permitted—they are intended to provide a consistent information security approach across all agencies, while meeting the mission-specific needs of each agency. Thus, agencies would be required to categorize their information and information systems according to control objectives and risk levels and to meet the minimum information security requirements.

Reporting Information to the Congress

H.R. 3844 seeks to improve accountability and congressional oversight by clarifying agency reporting requirements and ensuring that the Congress and GAO have access to information security evaluation results. In particular, it requires agencies to submit an annual report to both OMB and the comptroller general. This reporting requirement is in addition to the requirement in both GISRA and H.R. 3844 that IGs report the results of independent evaluations to OMB and would help to ensure that the Congress receives the information it needs for oversight of federal information security and related budget deliberations. However, to ensure that agencies provide consistent and meaningful information in their

reports, it would be important that any such reporting requirement consider specifying what these reports should address.

As reported in our March 2002 testimony, during first-year implementation of GISRA, OMB informed the agencies that it considered GISRA material the CIOs prepared for OMB to be predecisional and not releasable to the public, the Congress, or GAO.[16] OMB also considered agencies' corrective action plans to contain predecisional budget information and would not authorize agencies to release them to us. Later, OMB did authorize the agencies to provide copies of their executive summaries, and through continued negotiations with OMB since our March testimony, many agencies are now providing us with the more detailed information that they submitted to OMB. We are continuing to work with OMB to obtain appropriate information from agencies' first-year GISRA corrective action plans and to develop a process whereby this information can be routinely provided to the Congress in the future.

The Congress should have consistent and timely information for overseeing agencies' efforts to implement information security requirements and take corrective actions, as well as for budget deliberations. In our report being released today, we recommend that OMB authorize the heads of federal departments and agencies to release information from their corrective action plans to the Congress and GAO that would (1) identify specific weaknesses to be addressed, their relative priority, the actions to be taken, and the timeframes for completing these actions and (2) provide their quarterly updates on the status of completing these actions.[17] In commenting on our recommendation, OMB stated that it recognizes Congress's oversight role regarding agencies' actions to correct information security weaknesses and is continuing to develop a solution for next year's reporting to provide to the Congress information on agencies' corrective actions. However, OMB believed that removing predecisional information from current year plans would be difficult and is not having the agencies prepare information on their current plans that would be releasable to the Congress. One way to help ensure that the Congress receives such information would be to specifically require that agencies report it to the Congress and GAO.

[16]GAO-02-470T, March 6, 2002.

[17]GAO-02-407, May 2, 2002.

Responsibilities for National Security Systems

In our March 2002 testimony, we reported that we were unable to obtain complete information on GISRA implementation for national security systems. Specifically, OMB did not summarize the overall results of the audits of the evaluations for national security systems in its report to the Congress,[18] and the director of central intelligence declined to provide information for our review. In this regard, our report being released today includes a recommendation that OMB provide the Congress with appropriate summary information on the results of the audits of the evaluations for information security programs for national security systems.

While we were unable to evaluate this aspect of GISRA implementation, H.R. 3844 proposes to modify GISRA in a number of ways to clarify the treatment of national security systems and to simplify statutory requirements while maintaining protection for the unique requirements of such systems within the risk management approach of the law.

First, the bill replaces GISRA's use of the term "mission critical system." Instead, H.R. 3844 uses the traditional term "national security system," maintaining the longstanding statutory treatment of military and intelligence mission-related systems and classified systems.[19] It would also eliminate a separate category of systems included in GISRA's definition of mission critical system—debilitating impact systems—that broadened the exemption from GISRA for these systems.[20]

Second, consistent with the traditional definitions of national security systems, H.R. 3844 provides more straightforward distinctions between national security and non–national-security systems. This simplifies the law and could simplify compliance for agencies operating national security systems. The bill, for example, replaces GISRA's delegation of policy and oversight responsibilities for national security systems from OMB to

[18]Office of Management and Budget, *FY 2001 Report to the Congress on Federal Government Information Security Reform*, February 2002.

[19]This two-part definition includes (1) the national security system definition for military and intelligence mission-related systems, and (2) the classified system definition for systems that are protected at all times by procedures established for information that has been appropriately authorized to be kept secret in the interest of national defense or foreign policy.

[20]GISRA defines debilitating impact systems as systems that process information, "the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of the agency."

national security agencies by simply continuing longstanding limitations on OMB and NIST authority over national security systems.

Third, H.R. 3844 makes a number of changes to GISRA to streamline agency evaluation requirements that affect national security systems:

- The bill clarifies procedures for evaluating national security systems within the context of agencywide evaluations.
- The results of the evaluations of national security systems, not the evaluations themselves, are to be submitted to OMB, which will then prepare a summary report for the Congress. As in GISRA, the actual evaluations and any descriptions of intelligence-related national security systems are to be made available to the Congress only through the intelligence committees.
- The requirement for an audit of the evaluation of national security systems is eliminated. Instead, agencies are required to provide appropriate protections for national security information and, as discussed above, submit only the results of the evaluations to OMB.

We agree that these changes provide a more traditional definition of national security systems, and that such systems should be appropriately considered within the context of a comprehensive evaluation of agency information security. We also believe that requirements for reporting evaluation results to OMB and for OMB to prepare a summary report for the Congress would provide information needed for congressional oversight. This reporting requirement is consistent with our recommendation contained in the report that we are issuing today: that OMB provide the Congress with appropriate summary information on evaluation results for national security systems.

Additional Agency Requirements to Strengthen Information Security Programs

A number of provisions in the proposed legislation establish additional requirements for federal agencies that we believe would strengthen implementation and management of their information security programs. Some of the more significant requirements are as follows:

- Agencies would be required to comply with all standards applicable to their systems, including the proposed mandatory minimum control requirements and those for national security systems. Thus, in implementing an agencywide risk-management approach to information security, agencies with both national security and non–national-security systems would need to have an agencywide information security program that can address the security needs and standards for both kinds of systems.

- Under the bill, the requirement for designating a senior agency information security officer is more detailed than that under GISRA. This official is to (1) carry out the CIO's responsibilities under the act; (2) possess appropriate professional qualifications; (3) have information security as his or her primary duty; and (4) head an information security office with the mission and resources needed to help ensure agency compliance with the act.
- H.R. 3844 also requires each agency to document its agencywide security program and prepare subordinate plans as needed for networks, facilities, and systems. GISRA uses both the terms "security program" and "security plan" and does not specifically require that the program be documented. Our guidance for auditing information system controls states that entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it.[21]
- H.R. 3844 stresses the importance of agencies having plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. Such plans, procedures, and other service continuity controls are important because they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life. GAO and IG audit work indicate that most of the 24 large agencies we reviewed had weaknesses in service continuity controls, such as plans that were incomplete or not fully tested.

Updating the Mission of NIST and Its Advisory Board

H.R. 3844 maintains NIST's standards development mission for information systems, federal information systems, and federal information security (except for national security and classified systems), but updates the mission of NIST. Some of H.R. 3844's more significant changes to NIST's role and responsibilities would require NIST to:

[21]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

- develop mandatory minimum information security requirements and guidance for detecting and handling of information security incidents and for identifying an information system as a national security system;
- establish a NIST Office for Information Security Programs to be headed by a senior executive level director; and
- report annually to OMB to create a more active role for NIST in governmentwide information security oversight and to help ensure that OMB receives regular updates on the state of federal information security.

In addition, H.R. 3844 would revise the National Institute of Standards and Technology Act to rename NIST's Computer System Security and Privacy Advisory Board as the Information Security Advisory Board and to ensure that this board has sufficient independence and resources to consider information security issues and provide useful advice to NIST. The bill would strengthen the role of the board by (1) mandating that it provide advice not only to NIST in developing standards, but also to OMB who promulgates such standards; (2) requiring that it prepare an annual report; and (3) authorizing it to hold its meetings where and when it chooses.

Other Changes to Clarify and Streamline the Law

Our analysis of H.R. 3844 identified other proposed changes and requirements that could enhance federal information security, as well as help improve compliance by clarifying inconsistent and unclear terms and provisions, streamlining a number of GISRA requirements, and repealing duplicative provisions in the Computer Security Act and the Paperwork Reduction Act. These changes include the following:

Information security: H.R. 3844 would create a definition for the term "information security" to address three widely accepted objectives—integrity, confidentiality, and availability. Including these objectives in statute highlights that information security involves not only protecting information from disclosure (confidentiality), but also protecting the ability to use and rely on information (availability and integrity).

Information technology: H.R. 3844 would retain GISRA's use of the Clinger-Cohen Act definition of "information technology." However, H.R. 3844 clarifies the scope of this term by using consistent references to "information systems used or operated by any agency or by a contractor of an agency or other organization on behalf of an agency." This emphasizes that H.R. 3844 is intended to cover all systems used by or on behalf of agencies, not just those operated by agency personnel. As discussed previously, both OMB's and GAO's analyses of agencies' first-year GISRA

reporting showed significant weaknesses in information security management of contractor-provided or -operated systems.

Independent evaluations: The legislation would continue the GISRA requirement for an annual independent evaluation of each agency's information security program and practices. However, several language changes are proposed to clarify this requirement. For example, the word "representative" would be substituted for "appropriate" in the requirement that the evaluation involve the examination of a sample of systems or procedures. In addition, the bill would also require that the evaluations be performed in accordance with generally accepted government auditing standards, and that GAO periodically evaluate agency information security policies and practices. We agree with these proposed changes to independent evaluations, but as noted in our March 2002 testimony, these evaluations and expanded coverage for all agency systems under GISRA and H.R. 3844 place a significant burden on existing audit capabilities and require ensuring that agency IGs have necessary resources to either perform or contract for the needed work.[22]

Federal information security incident center: The bill would direct OMB to oversee the establishment of a central federal information security incident center and expands GISRA references to this function. While not specifying which federal agency should operate this center, H.R. 3844 specifies that the center would

- provide timely technical assistance to agencies and other operators of federal information systems;
- compile and analyze information security incident information;
- inform agencies about information security threats and vulnerabilities; and
- consult with national security agencies and other appropriate agencies, such as an infrastructure protection office.

H.R. 3844 would also require that agencies with national security systems share information security information with the center to the extent consistent with standards and guidelines for national security systems. This provision should encourage interagency communication and consultation, while preserving the discretion of national security agencies to determine appropriate information sharing.

[22]GAO-02-470T, March 6, 2002.

Technical and conforming amendments. In addition to its substantive provisions, H.R. 3844 would make a number of minor changes to GISRA and other statutes to ensure consistency within and across these laws. These changes include the elimination of certain provisions in the Paperwork Reduction Act and the Computer Security Act that are replaced by the requirements of GISRA and H.R. 3844.

Improvements Underway, But Challenges to Federal Information Security Remain

As discussed previously, GISRA established important program, evaluation, and reporting requirements for information security; and the first-year implementation of GISRA has resulted in a number of important administration actions and significant agency benefits. In addition, H.R. 3844 would continue and strengthen these requirements to further improve federal information security. However, even with these and other information security-related improvement efforts undertaken in the past few years—such as the president's creation of the Office of Homeland Security and the President's Critical Infrastructure Protection Board—challenges remain.

Given the events of September 11, and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed in the context of the broader array of risks to the nation's welfare. Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement. In 1998, shortly after the initial issuance of Presidential Decision Directive (PDD) 63 on protecting the nation's critical infrastructure, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the assistant to the president for national security affairs work together to ensure that the roles of new and existing federal efforts were coordinated under a comprehensive strategy.[23] Our later reviews of the National Infrastructure Protection Center and of broader federal efforts to counter computer-based attacks showed that

[23]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*. GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).

there was a continuing need to clarify responsibilities and critical infrastructure protection objectives.[24]

As I emphasized in my March 2002 testimony, as the administration refines the strategy that it has begun to lay out in recent months, it is imperative that it take steps to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed.[25] These steps would include the following:

- It is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security, and NIST, with assistance from the National Security Agency, is responsible for establishing related standards. In addition, interagency bodies—such as the CIO Council and the entities created under PDD 63 on critical infrastructure protection—are attempting to coordinate agency initiatives. Although these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not yet taking place. Further, it is unclear how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.
- Ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA and H.R. 3844, could allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and monitoring process established through these provisions, is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.
- Agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the

[24]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities.* GAO-01-323 (Washington, D.C.: Apr. 25, 2001); *Combating Terrorism: Selected Challenges and Related Recommendations.* GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

[25]GAO-02-470T, March 6, 2002.

federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

- Agencies can allocate resources sufficient to support their information security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.
- Expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As the director of the CERT® Coordination Center[26] testified before this subcommittee last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches." In addition, in its December 2001 third annual report, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the Gilmore Commission) recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.[27]

Concluding Observations

In summary, the first-year implementation of GISRA has resulted in a number of benefits and positive actions, but much work remains to be done to achieve the objectives of this legislation. Continued authorization of federal information security legislation is essential to sustain agencies' efforts to implement good security practices and to identify and correct significant weaknesses. This reauthorization will also help reinforce the federal government's commitment to establishing information security as

[26]CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[27] *Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, December 15, 2001.

an integral part of its operations, as well as help ensure that the administration and the Congress receive the information they need to effectively manage and oversee federal information security.

The changes in requirements, responsibilities, and legislative language proposed in H.R. 3844 would further strengthen the implementation and oversight of information security in the federal government, particularly in establishing mandatory minimum controls and creating reporting requirements to ensure that the Congress receives the information it needs for oversight and budget deliberations related to federal information security. In addition, other changes proposed by H.R. 3844 would clarify and streamline the law and could increase agency compliance with information security requirements. At the same time, with the increasing threat to critical federal operations and assets and poor federal information security, it is imperative that the administration and the agencies implement a comprehensive strategy for improvement that emphasizes information security and addresses known weaknesses.

Messrs. Chairmen, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittees may have at this time.

Contact

If you should have any questions about the testimony, please contact me at (202) 512-3317. I can be reached by e-mail at *daceyr@gao.gov*.

(310158)