GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 30, 2009

The Honorable Diane Watson
Chairwoman
The Honorable Brian Bilbray
Ranking Member
Subcommittee on Government Management, Organization, and Procurement
Committee on Oversight and Government Reform
House of Representatives

Subject: *Federal Information Security Issues*

This letter responds to your request that I address additional questions arising from the May 19, 2009, hearing on federal information security held by the Subcommittee on Government Management, Organization, and Procurement. In that hearing, we discussed the current state of information security throughout the federal government and agency efforts to comply with the requirements of the Federal Information Security Management Act of 2002 (FISMA).[1] Your questions, along with our responses, follow.

1. Please comment on the need for improved cyber security relating to S.773, the proposed Cybersecurity Act of 2009.[2]

The bill is intended to improve cyber security in the United States. According to the bill, America's failure to protect cyberspace is one of the most urgent national security problems facing the country.

The need for improved cyber security in the federal government is clear. Since 1997, we have designated federal information security as a governmentwide high-risk area in our biennial reports to Congress.[3] Recently, we testified that reviews at the 24

[1] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).
[2] S.773, introduced April 1, 2009, by Senator Rockefeller for himself, Senator Snowe, and Senator Nelson of Florida.
[3] Most recently, GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

major federal agencies[4] continue to highlight deficiencies in their implementation of information security policies and procedures.[5] For example, in their fiscal year 2008 performance and accountability reports, 20 of the 24 the agencies noted that inadequate information system controls were either a material weakness or a significant deficiency.[6] In addition, 23 of the 24 agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. Furthermore, those agencies also had weaknesses in their agencywide information security programs.

In March 2009,[7] we testified that the present cyber security strategy and its implementation had not been fully effective in mitigating the threat. As an example, the number of incidents reported by federal agencies has increased dramatically over the past 3 years, tripling from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008.

We have previously made recommendations on the steps necessary for improving cyber security, and nationally recognized experts have identified improvements aimed at strengthening the strategy and, in turn, the nation's cyber security posture. These improvements include developing a national strategy that clearly articulates strategic objectives, goals, and priorities; establishing White House leadership; publicizing and raising awareness about the seriousness of the cyber security problem; focusing more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans; bolstering public/private partnerships through an improved value proposition and use of incentives; focusing greater attention on addressing the global aspects of cyberspace; placing greater emphasis on cyber security research and development, including consideration of how to better coordinate government and private sector efforts; and increasing the cadre of cyber security professionals. Until these improvements are considered, our nation's federal and private sector infrastructure systems remain at risk of not being adequately protected.

---

[4] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[5] GAO, *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist*, GAO-09-701T (Washington, D.C.: May 19, 2009).

[6] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

[7] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington D.C.: Mar. 10, 2009).

2. Please provide recommendations to improve the Federal Information Security Management Act.

FISMA was intended to provide (1) a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and (2) a mechanism for improved oversight of federal agency information security programs. To do this, the act requires agencies to develop, document, and implement an agencywide information security program that is largely consistent with the principles noted in our study of the risk management activities of leading private sector organizations[8]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and controls effectiveness. The act also requires annual reports and independent annual evaluations on the adequacy and effectiveness of agency information security policies, procedures, and practices, and compliance with the provisions of the act. In addition to the improvements noted in our response to the prior question, we believe the following suggestions can improve FISMA and its associated implementing guidance can be improved with the following actions.

Clarify requirements for testing and evaluating security controls. Agencies are required to test and evaluate the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls on information systems. However, as we have previously reported,[9] federal agencies have not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Clarifying or strengthening FISMA and its implementing guidance for determining the frequency, depth, and breadth of security control tests and evaluations could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations, and assets.

Require agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program. FISMA requires that agencies report annually to Congress on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with FISMA requirements. The intent of the FISMA reporting requirements was to provide Congress with a bottom line on whether the agencies' information security programs are effective. In the initial years of FISMA implementation, the metrics required by Office of Management and Budget (OMB) reporting instructions served an important role in measuring progress to implement the most basic FISMA requirements: for example, whether risk assessments or contingency plan testing was performed. However, as we and others have reported, the metrics do not adequately measure the effectiveness of agencies' information security programs. Therefore, FISMA can be improved by requiring that agency management include in its annual report an assurance statement on the overall adequacy and effectiveness of information

[8] GAO, *Executive Guide: Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).
[9] GAO, *Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, GAO-07-65 (Washington, D.C.: Oct. 20, 2006).

security within the agency. Such assurance statements should include an identification and analysis of significant deficiencies in information security, and should consider the impact of deficiencies identified in the agency's remedial action plans. Similar management assurance statements are currently required under OMB Circular A-123, for agency internal controls under the Federal Managers' Financial Integrity Act of 1982,[10] and for controls over financial reporting at public companies under the Sarbanes-Oxley Act[11]

Enhance independent annual evaluations. FISMA also requires an annual independent evaluation of each agency's information security program and practices to determine the effectiveness of such program and practices. However, according to our annual analysis of FISMA reports and our information security work, such independent evaluations lack a common approach and culminate in disparities in type of work conducted, scope, methodology, and content. The use of generally accepted government auditing standards to perform the independent evaluations, already in place at 13 of the 24 major departments and agencies, would provide a baseline for consistent evaluations and help ensure their quality. In addition, independent review and analysis of management's assurance statement, discussed above, as part of the independent evaluation would provide important information to Congress about the quality of management's assurance statement. Therefore, FISMA can be improved by specifically requiring that the independent evaluation be conducted in accordance with government auditing standards and include (1) an assessment of management's process for developing the conclusions in the assurance statement, (2) an identification of any significant deficiencies in management's process, and (3) a statement about whether, based on the independent evaluation, there are any significant disagreements with management's conclusions on the overall adequacy and effectiveness of information security within the agency.

Strengthen annual reporting mechanisms. As we have previously reported,[12] OMB's reporting instructions for fiscal year 2008 do not sufficiently address several processes key to implementing an agencywide security program and are sometimes unclear. For example, the reporting instructions do not request inspectors general to provide information on the quality or effectiveness of agencies' processes for developing and maintaining inventories, providing specialized security training, and monitoring contractors. In prior reports,[13] we have also recommended that OMB develop additional performance metrics that measure the effectiveness of FISMA activities, such as requiring agencies to report on patch management and ensuring that all aspects of key FISMA requirements are reported on in the annual reports. We are currently reviewing the use of metrics to guide and monitor information security control activities at federal agencies and at leading nonfederal organizations.

---

[10] Federal Managers' Financial Integrity Act of 1982, Pub. L. No. 97-255 (Sept. 8, 1982), 31 U.S.C. 3512.
[11] Sarbanes-Oxley Act, Pub. L. No. 107-204 (July 30, 2002), 15 U.S.C. 7262.
[12] GAO, *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist*, GAO-09-701T (Washington, D.C.: May 19, 2009).
[13] GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007), and *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

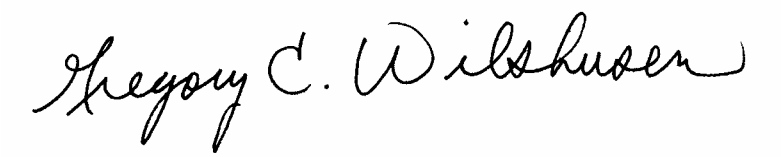
OMB can also improve FISMA reporting by fully summarizing the findings from the inspectors general independent evaluations to identify significant deficiencies in agencies' information security practices. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices.

Strengthen OMB oversight of agency information security programs. As we have previously testified,[14] OMB does not explicitly approve or disapprove agencies' information security programs. FISMA requires OMB to review agencies' information security programs at least annually, and approve or disapprove them. This mechanism for establishing accountability and holding agencies accountable for implementing effective security programs was not used. Implementation of this mechanism can provide additional oversight.

- - - - -

We are sending copies of this letter to the Chairwoman and Ranking Member of the House Subcommittee on Government Management, Organization, and Procurement. In addition, this letter will be available at no charge on GAO's Web site at http://www.gao.gov.

In responding to these questions, we relied on previous audit work we performed in developing prior reports and testimonies regarding protection of critical infrastructure and federal agency implementation of FISMA. We conducted our work in support of this letter during May and June 2009. The work on which this letter is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. If you have any questions regarding this letter, please contact me at (202) 512-6244 or wilshuseng@gao.gov. GAO staff who made major contributions to this letter are Robert Dacey (Chief Accountant), Charles Vrabel (Assistant Director), Larry Crosland, Nancy Glover, David Plocher, and Jayne Wilson.



Gregory C. Wilshusen
Director, Information Security Issues

(311029)

[14] GAO-09-701T.