



G A O

Accountability \* Integrity \* Reliability

United States General Accounting Office  
Washington, DC 20548

---

April 16, 2002

The Honorable Stephen Horn  
Chairman, Subcommittee on Government Efficiency,  
Financial Management and Intergovernmental Relations  
Committee on Government Reform  
House of Representatives

Subject: *Information Security: Subcommittee Post-Hearing Questions Concerning the  
Additional Actions Needed to Implement Reform Legislation*

This letter responds to your March 26, 2002, request that we provide answers to questions relating to our testimony of March 6, 2002.<sup>1</sup> In that hearing, we discussed efforts by the Office of Management and Budget (OMB), 24 of the largest federal agencies, and these agencies' inspectors general to implement requirements and report evaluation results according to provisions for Government Information Security Reform (the reform provisions) that were enacted as part of the National Defense Authorization Act for Fiscal Year 2001.<sup>2</sup> Your questions, along with our responses, follow.

1. *Do you agree with OMB's assessment of the top six security weaknesses within the Federal agencies? Why or why not?*

We agree that the six security weaknesses OMB identified in its report to the Congress represent significant deficiencies in federal departments' and agencies' information security programs. Specifically, these are (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

However, as OMB indicates, for the most part, its report focuses on management issues, not those of technical or operational implementation. As pointed out in my written statement, our analyses of the reports submitted to OMB by 24 of the largest federal agencies and their inspectors general showed that there are other key security requirements of the reform provisions that agencies have not fully implemented, such as those that require periodic risk assessments for all agency systems and periodic testing and evaluation of controls to ensure

---

<sup>1</sup>U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Provisions*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

<sup>2</sup>Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L.106-398 (Oct. 30, 2000).

that they are implemented and operating as intended. In addition, our analyses of GAO and inspector general audit reports issued from July 2000 through September 2001 confirm that most agencies have significant weaknesses in their information security 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. In particular, we found that for the 24 large federal departments and agencies we reviewed, all had significant weaknesses in *security program management*, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented, and in *access controls*, which ensure that only authorized individuals can read, alter, or delete data.

2. *In your statement, you indicated that “an important step toward ensuring information security is to fully understand the weaknesses that exist, and as the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.”*

- *Why are security weaknesses in Federal information systems still not fully understood?*

In past years, most reviews of information security controls were performed as part of agency financial statement audits and, thus, focused on financial systems. However, since the reform provisions are applicable to essentially all systems including national security systems and other types of risk beyond financial statements, audit coverage, as well as the required annual management reviews of agency information security programs, should include such additional risks and more nonfinancial systems. This is particularly true for agencies with significant nonfinancial operations, such as the departments of Defense and Justice. It is the extent of the weaknesses for these nonfinancial systems that are still not fully identified.

- *Is there any way to characterize the impact of those undiscovered weaknesses?*

While we do not know the extent of the weaknesses in many nonfinancial systems, any weaknesses would likely be similar to those found in financial systems. Such weaknesses are categorized within six general control categories, which are described in GAO's *Federal Information System Controls Audit Manual*.<sup>3</sup> These general control categories are (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.

My written statement characterizes the impact of such control weaknesses as placing a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;

---

<sup>3</sup>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).

- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information—such as taxpayer data, social security records, medical records, and proprietary business information—could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Until these undiscovered weaknesses are fully identified, corrective actions will not be fully effective.

- *Are current evaluation and audit methodologies adequate to uncover these weaknesses?*

While adequate methodologies currently exist to identify and detect information security weaknesses, such methodologies must be appropriately applied to provide necessary audit and management review coverage. Further, periodically evaluating the effectiveness of security policies and controls is essential to ensuring that controls are implemented and functioning as intended. For example, GAO's *Federal Information System Controls Audit Manual* provides a methodology for evaluating information system controls. However, audit coverage should be expanded to cover both financial and nonfinancial systems. This will place a significant new burden on the existing audit capabilities of agency inspectors general and will require that they have appropriate resources to either perform or contract for the needed work. As another example, the reform provisions require program officials to perform annual program reviews, which are to include periodic testing and evaluation of the effectiveness of information security policies, procedures, controls, and techniques. To help perform these reviews, the National Institute of Standards and Technology developed its *Federal IT Security Assessment Framework*,<sup>4</sup> which uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. While many of the 24 agencies we contacted said that they used this questionnaire in performing their reviews, many also said that their results were based on management self-assessments, which did not include control testing to ensure that information security controls were implemented and operating as intended.

3. *What do you see as the most significant barriers to securing Federal information technology resources? What can be done to overcome these barriers?*

Through our audit work and analyses, we have noted several significant barriers to securing federal information technology resources. Three such barriers—poor information security program management, obtaining appropriate funding, and acquiring needed technical and audit expertise—are discussed below.

---

<sup>4</sup>National Institute of Standards and Technology, *Federal Information Technology Security Assessment Framework*, prepared for the Federal CIO Council by the NIST Computer Security Division Systems and Network Security Group (Nov. 28, 2000).

### *Poor Information Security Program Management*

GAO and inspector general audit work reviewed for 24 of the largest federal agencies indicates that a significant barrier to securing federal information technology resources is agencies not fully implementing a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost-effective manner rather than reacting to individual problems in an ad-hoc manner only after a problem has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed security plans for major systems based on risk, (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on ineffective controls, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

### *Obtaining Appropriate Funding*

Another barrier frequently mentioned by agencies is obtaining appropriate information security funding. However, while OMB requires agencies to identify amounts for information security in their budget submissions, agencies do not always provide this information. For example, the fiscal year 2001 and 2002 security costs that OMB requested agencies to identify as part of their reform provision reporting were not provided in some cases, and in other cases, there was no detail as to what these costs consisted of or how they are actually reflected in agency budget submissions. Further, OMB reports that it assessed the agencies' performance against the amount agencies spent and did not find that increased security spending equals increased security performance. As a result, OMB concludes that there is no evidence that poor security is a result of lack of money.

To help overcome this funding barrier, agencies must identify their information security costs to demonstrate their understanding of such costs and justify continued or additional funding. Further, as OMB indicates in its report to the Congress, much can also be done to cost-effectively address common weaknesses, such as security training, across government rather than piecemeal by agency. New funding initiatives by the administration may also help provide additional information security resources to federal agencies. For fiscal year 2003, the president is requesting \$4.2 billion for information security funding from a total information technology investment request of approximately \$52 billion as compared to about \$2.7 billion reported for fiscal year 2002 from a total reported information technology investment of about \$48 billion. This fiscal year 2003 amount does not include new governmentwide initiatives of the Office of Homeland Security, which include \$298 million for cyberspace security.

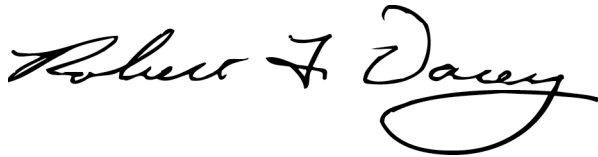
*Acquiring Technical and Audit Expertise*

As highlighted during the Year 2000 challenge, the availability of technical and audit expertise is a continuing concern to agencies. Agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Programs are now underway to increase these resources by encouraging the creation of and participation in information security curriculums in educational institutions. In addition, the federal government must also maximize the value of its technical staff by sharing expertise and information.

---

We are sending copies of this letter to OMB and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-3317. I can also be reached by e-mail at [dacey@gao.gov](mailto:dacey@gao.gov).

Sincerely yours,

A handwritten signature in black ink that reads "Robert F. Dacey". The signature is written in a cursive style with a large, looping flourish at the end of the name.

Robert F. Dacey  
Director, Information Security Issues