United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at time 1:00 p.m. EDT
Thursday, April 19, 2007

INFORMATION SECURITY

Persistent Weaknesses Highlight Need for Further Improvement

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO

Accountability * Integrity * Reliability

April 19, 2007

INFORMATION SECURITY

Persistent Weaknesses Highlight Need for Further Improvement

GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-751T, a testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security are a widespread problem with potentially devastating consequences—such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information. In reports to Congress since 1997, GAO has identified information security as a governmentwide high-risk issue.

Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies. FISMA also defines responsibilities for ensuring centralized compilation and analysis of incidents that threaten information security and providing timely technical assistance in handling security incidents.

In this testimony, GAO discusses the continued weaknesses in information security controls at 24 major federal agencies, the reporting and analysis of security incidents, and efforts by the Department of Homeland Security (DHS) to develop a cyber threat analysis and warning capability.

GAO based its testimony on its previous work in this area as well as agency and congressional reports.

www.gao.gov/cgi-bin/getrpt?GAO-07-751T.

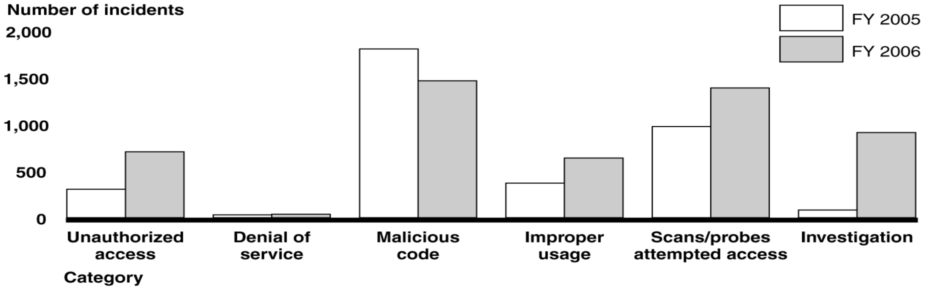
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In their fiscal year 2006 financial statement audit reports, 21 of 24 agencies indicated that they had significant weaknesses in information security controls. As shown by reports by GAO and agency inspectors general (IG), the weaknesses persist in major categories of controls—including, for example, access controls, which ensure that only authorized individuals can read, alter, or delete data, and configuration management controls, which provide assurance that only authorized software programs are implemented. An underlying cause for these weaknesses is that agencies have not yet fully implemented agencywide information security programs, which provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent unauthorized use, disclosure, and modification.

Organizations can reduce the risks associated with intrusions and misuse if they take steps to detect and respond to incidents before significant damage occurs, analyze the causes and effects of incidents, and apply the lessons learned. As part of this process, federal policy requires agencies to report incidents to the federal information security incident center—US-CERT (Computer Emergency Readiness Team). According to US-CERT, federal agencies reported a record number of incidents in fiscal year 2006. As the figure shows, since 2005, the number of incidents reported increased in every category except one. However, inconsistencies exist in reporting at various levels. If agencies do not properly capture and analyze security incidents, they risk losing valuable information needed to prevent future exploits and understand the nature and cost of security threats.

Strategic analysis and warning is an essential element of assisting agencies in addressing information security incidents. GAO has recommended that DHS develop such a capability for addressing cyber attacks. DHS has established various initiatives to enhance its analytical capabilities through US-CERT and GAO believes with continued progress in addressing strategic analysis and warnings, US-CERT can further agencies' efforts to reduce risks associated with incidents.



Source: GAO analysis of OMB data.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing to discuss information security over federal systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Proper safeguards are essential to protect systems from attackers attempting to gain access and obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems.

For many years, we have reported that poor information security is a widespread problem with potentially devastating consequences. In reports to Congress since 1997, we have identified information security as a governmentwide high-risk issue.[1] Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[2] which permanently authorized and strengthened the information security program, evaluation, and annual reporting requirements for federal agencies.

In our testimony today, we will summarize (1) the continued weaknesses in information security controls at federal agencies, (2) federal agencies' reporting of information security incidents, and (3) efforts by the Department of Homeland Security (DHS) to develop a cyber threat warning and analysis capability. In preparing for this testimony, we relied on our previous reports on information security at federal agencies and the challenges

[1] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[2] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

faced by DHS in fulfilling its cybersecurity responsibilities. We also analyzed agencies' Inspector General (IG) reports pertaining to information security; congressional reports; the 24 major federal agencies' FISMA reports for fiscal years 2004, 2005, and 2006; the performance and accountability reports for those agencies; and the Office of Management and Budget's FISMA guidance and mandated annual reports to Congress. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Significant information security weaknesses continue to place federal agencies at risk. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies cited information security control weaknesses. An underlying cause for these weaknesses is that agencies have not fully implemented agencywide information security programs. These weaknesses persist even as many agencies report increased implementation of information security program activities. However, until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be sufficiently safeguarded to prevent unauthorized use, disclosure, and modification.

In 2006, agencies reported a record number of information security incidents to US-CERT (Computer Emergency Readiness Team)—the DHS unit responsible for collecting such information. At the same time, although agencies have noted improvements in incident reporting procedures, inconsistencies exist across agencies. For example, one agency reported no incidents to US-CERT, although it reported more than 800 incidents internally and to law enforcement authorities. IGs have also reported weaknesses in agencies' incident reporting procedures.

In addition to its incident reporting activities with US-CERT, DHS has taken steps towards addressing prior recommendations for developing a strategic analysis and warning capability for cyber attacks. Specifically, DHS has established various initiatives to enhance its analytical capabilities, including intelligence sharing through US-CERT and situational awareness tools at selected federal agencies. We believe that with continued progress in addressing strategic analysis and warnings, US-CERT can further agencies' efforts to reduce risks associated with incidents. However, DHS has not yet fully implemented our original recommendations, particularly in implementing such a capability beyond the federal environment.

Background

Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is high. For example, resources (such as federal payments and collections) could be lost or stolen, data could be modified or destroyed, and computer resources could be used for unauthorized purposes or to launch attacks on other computer systems. Sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting national defense and emergency services. Finally, agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Recognizing the importance of securing federal systems and data, Congress passed FISMA, which set forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA also defined several public sector responsibilities that have been assumed by US-CERT, a partnership between DHS and the public and private sectors that was established in 2003 to coordinate defense against and responses to cyber attacks across the nation.[3] US-CERT's responsibilities include compiling and analyzing information about incidents that threaten information security and providing timely technical assistance regarding security incidents.

Significant Weaknesses Continue to Place Federal Agencies at Risk

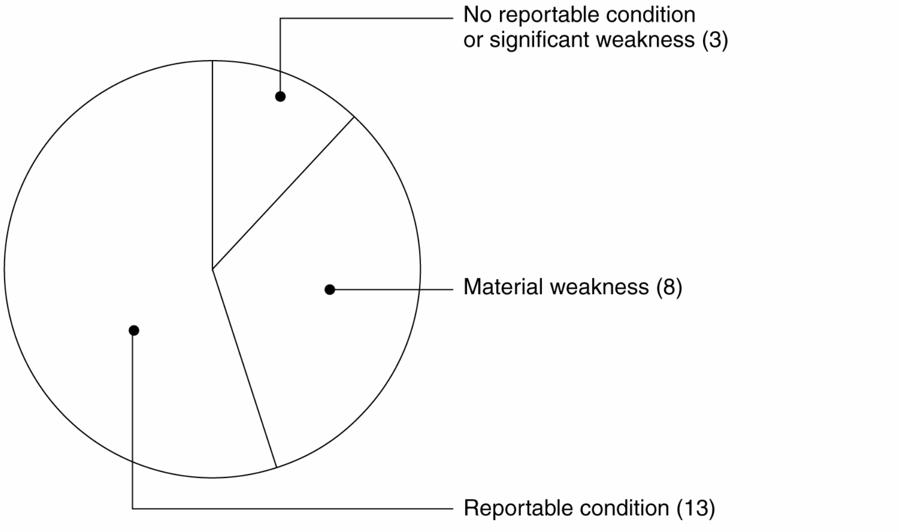
Significant weaknesses continue to threaten the confidentiality, integrity and availability of federal information and information systems. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies indicated that deficient information security controls were either a reportable condition[4] or material weakness (see fig. 1).[5]

[3] FISMA charged the Director of OMB with ensuring the operation of a federal information security center. The required functions are performed by US-CERT, which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.

[4] Reportable conditions are significant deficiencies in the design or operation of internal control that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

[5] A material weakness is a reportable condition that precludes the entity's internal control from providing reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

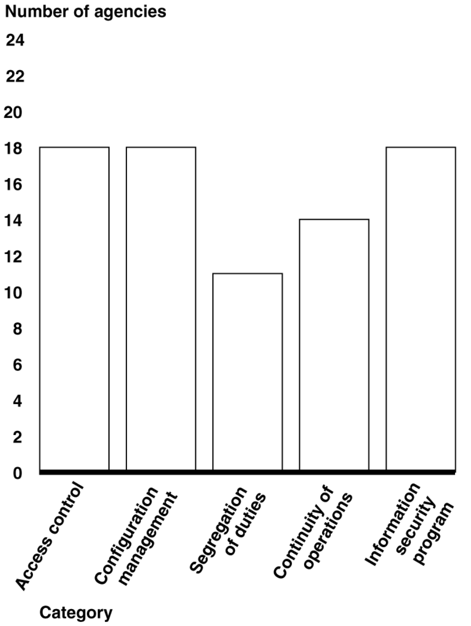
Figure 1: Agencies Reporting of Information Security Controls in Fiscal Year 2006 Financial Statement Audits



Source: GAO analysis.

These persistent weaknesses appear in the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Figure 2 shows how many of the agencies had weaknesses in these five areas.

Figure 2: Information Security Weaknesses at the 24 Major Agencies for Fiscal Year 2006



Source: GAO analysis.

Access Controls Were Not Adequate

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, can be both electronic and physical. Electronic access controls include use of passwords, access privileges, encryption, and audit logs. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft.

Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate access controls in place to ensure that only authorized individuals could access or manipulate data. Of the 24 major agencies, 18 had access control weaknesses. Such weaknesses included not replacing well-known vendor-supplied passwords, permitting excessive access privileges that users did not need to perform their jobs, not encrypting sensitive information, and not creating or maintaining adequate audit logs. Agencies also lacked effective physical security controls. For instance, many of the data losses that occurred at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Shortcomings Existed in Other Controls

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of information. These controls include policies, procedures, and techniques addressing configuration management to ensure that software patches are installed; appropriately segregating incompatible duties; and establishing service continuity planning. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

Federal agencies demonstrated weaknesses in these control areas. For example, several agencies did not always consistently install critical software patches in a timely manner, segregate duties such as security and system administration, or adequately update and test contingency plans.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for the information security weaknesses identified at federal agencies is that they have not yet fully implemented agencywide information security programs. An agencywide security program provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, promoting awareness, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources.

In their annual FISMA reports for fiscal year 2006, agencies reported increased compliance in several security program elements required by the law or federal policy. For example, agencies reported increases in the percentages of systems with assigned risk levels, employees receiving security awareness training, systems that have been certified and accredited[6] and systems whose security controls were tested and evaluated.

However, our reports and those of agency IGs indicate that at least 18 of the 24 major agencies had not fully implemented agencywide programs. For example, agencies often did not effectively ensure that all employees and contractors, including those with significant information security responsibilities, received sufficient training. Also, 10 IGs rated the quality of their agencies' certification and accreditation process as "poor" or "failing" and continued to identify specific weaknesses with the process, such as incomplete risk assessments and security plans. We have also identified shortcomings in agencies' efforts in testing and evaluating the effectiveness of their information security controls. In 2006, we reported that agencies had not adequately designed and effectively implemented policies for performing such tests and evaluations.[7] Policies often did not include elements important for performing effective testing. In addition, at agencies where we examined the effectiveness of security controls, we found that they did not identify many of the vulnerabilities we identified on their systems. Further, for case studies of 30 systems at six agencies, weaknesses included insufficient testing documentation, inadequately defined assessment methods, inadequate security testing, and lack of

[6] OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

[7] GAO, *Information Security: Agencies Need to Develop and Implement Policies for Periodic Testing*, GAO-07-65 (Washington, D.C.: Oct. 20, 2006).

remedial actions included in testing plans. Finally, for 16 of 24 major agencies, IGs were not able to provide assurance that their agencies almost always incorporated weaknesses for all systems into their remediation plans. Our reviews have also reported that weaknesses were not always resolved as reported, and agencies' remedial action plans did not identify resources necessary to correct weaknesses and were not always updated.

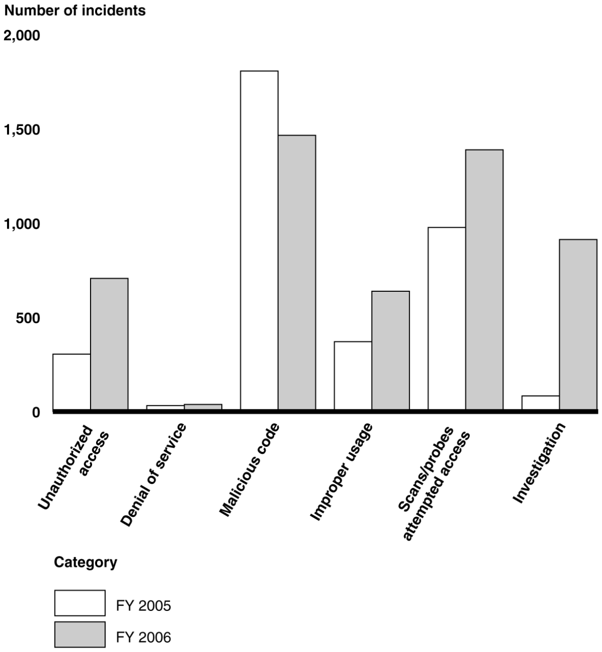
As a result, agencies do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of the agency. Furthermore, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent unauthorized use, disclosure, and modification.

Incident Reporting Varies Across Agencies

Although strong controls may not block all intrusions and misuse, organizations can reduce the associated risks if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an organization to improve its understanding of security threats and potential costs of security incidents, as well as pinpointing vulnerabilities that need to be addressed so that they are not exploited again. When incidents occur, agencies are to notify the federal information security incident center—US-CERT.

According to the US-CERT annual report for fiscal year 2006, federal agencies reported a record number of incidents, with a notable increase in incidents reported in the second half of the year. As figure 3 shows, since 2005, the number of incidents reported to US-CERT increased in every category except for malicious code. Further, a 2006 report by the House Committee on Government Reform illustrated that agencies have a wide range of incidents involving loss or theft and privacy breaches.[8] The report further indicates that the loss of personally identifiable information occurs governmentwide and is not limited to the well-publicized incident at the Department of Veterans Affairs (which involved information on about 26.5 million veterans and active duty military personnel).

Figure 3. Incidents Reported to US-CERT in FY05 and FY06



Source: GAO analysis of OMB data.

Although agencies have noted many improvements in incident reporting procedures, there are still inconsistencies in reporting at various levels. For example, one agency reported no incidents to US-CERT, although it reported more than 800 incidents internally and to law enforcement authorities. Several IGs also noted specific weaknesses in incident procedures such as components not reporting incidents reliably, information

[8] Committee on Government Reform, U.S. House of Representatives, *Staff Report: Agency Breaches Since January 1, 2003* (Washington, D.C.: Oct. 13, 2006).

being omitted from incident reports, and reporting time requirements not being met. Without properly accounting for and analyzing security problems and incidents, agencies risk losing valuable information needed to prevent future exploits and understand the nature and cost of threats directed at them.

DHS Is Acting to Implement GAO Recommendations on Strategic Analysis and Warning, But More Actions Needed

Strategic analysis and warning is an essential element of assisting agencies in addressing information security incidents. We have previously reported that developing and enhancing a national cyber analysis and warning capability is a key DHS cybersecurity responsibility.[9] Over the last several years, we have made recommendations to DHS—as the nation's focal point for cyber critical infrastructure protection—to develop a strategic analysis and warning capability for addressing cyber attacks.[10] Specifically, we recommended that responsible executive branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data.

DHS has taken steps towards addressing our recommendations. As we reported in 2005, DHS established various initiatives to enhance its analytical capabilities, including intelligence-sharing through US-CERT and situational awareness tools through the US-CERT Einstein program at selected federal agencies. The Einstein program provides an automated process for collecting, correlating, analyzing, and sharing computer security information across the federal civilian government. Einstein is

[9] GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

[10] GAO, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*, GAO-06-1087T (Washington, D.C.: Sept. 13, 2006).

currently deployed to nine federal agencies; US-CERT plans to deploy Einstein to an additional 10 to 15 agencies in fiscal year 2008, with a goal of deploying it to all cabinet level and critical independent federal agencies. According to DHS officials, Einstein has greatly reduced the time for the federal government to gather and share critical data on computer security risks (from 5 to 7 days to 4 to 5 hours). Further, the officials stated that Einstein has the potential to reduce data collection and information sharing to under 2 hours, allowing for vast improvements in governmental cyber response and recovery times. If properly implemented and expanded as planned, DHS's efforts in this program could strengthen its cyber threat analysis and warning capability. However, DHS has not yet fully implemented our original recommendations, particularly in implementing such a capability beyond the federal environment.

In summary, although agencies report increased compliance with security program activities required by FISMA and federal policy, serious weaknesses persist at federal agencies, and reported incidents are rising. The weaknesses exist, in part, because agencies have not fully implemented their information security programs. Until such programs are fully implemented, agencies will be at increased risk of exposure to cyber attacks. As agencies report record numbers of incidents, inconsistencies in reporting persist. With continued progress in addressing strategic analysis and warning, DHS's US-CERT can help agencies mitigate the risk associated with incidents.

Mr. Chairman, this concludes our statement. We would be happy to answer any questions at this time.

Contacts and Acknowledgements

If you have any questions regarding this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or David A. Powner at (202) 512-9286 or pownerd@gao.gov.

Other key contributors to this report include Scott Borre, Barbara Collier, Larry Crosland, Mike Gilmore, Min Hyun, Jeffrey Knott, Jayne Wilson, and Eric Winter.