United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees
Committee on Oversight and Government Reform
House of Representatives

For Release on Delivery
Expected at 11:30 am EST
Thursday, February 14, 2008

INFORMATION SECURITY

Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-08-496T

February 14, 2008

INFORMATION SECURITY

Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-496T, a testimony before congressional subcommittees, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Information security is especially important for federal agencies, where the public's trust is essential and poor information security can have devastating consequences. Since 1997, GAO has identified information security as a governmentwide high-risk issue in each of its biennial reports to the Congress. Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002, which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on the current state of federal information security and compliance with FISMA. This testimony summarizes (1) agency progress in performing key control activities, (2) the effectiveness of information security at federal agencies, and (3) opportunities to strengthen security. In preparing for this testimony, GAO reviewed prior audit reports; examined federal policies, guidance, and budgetary documentation; and analyzed agency and inspector general (IG) reports on information security.

To view the full product, including the scope and methodology, click on GAO-08-496T. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Over the past several years, federal agencies consistently reported progress in performing certain information security control activities. According to the President's proposed fiscal year 2009 budget for information technology, the federal government continued to improve information security performance in fiscal year 2007 relative to key performance metrics established by the Office of Management and Budget (OMB). The percentage of certified and accredited systems governmentwide reportedly increased from 88 percent to 92 percent. Gains were also reported in testing of security controls – from 88 percent of systems to 95 percent of systems – and for contingency plan testing – from 77 percent to 86 percent. These gains continue a historical trend that GAO reported on last year.

Despite reported progress, major federal agencies continue to experience significant information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by an increasing number of security incidents experienced by federal agencies.

Nevertheless, opportunities exist to bolster federal information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For example, OMB has established an information systems security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

Mr. Chairmen and Members of the Subcommittees:

Thank you for the opportunity to participate 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. Over the past few years, federal agencies have reported numerous security incidents in which sensitive information has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to a loss of privacy, identity theft, and other financial crimes.

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

In my testimony today, I will summarize (1) agencies' reported progress in performing key control activities, (2) the effectiveness of information security at federal agencies, including security incidents reported at federal agencies, and (3) opportunities to improve federal information security. In preparing for this testimony, we reviewed prior GAO and agency Inspector General (IG) reports on

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

information security at federal agencies. We also examined fiscal year 2007 governmentwide information security performance information presented in the President's proposed fiscal year 2009 budget for information technology, and information about federal security initiatives; analyzed performance and accountability reports for 24 major federal agencies;[3] and reviewed the Office of Management and Budget's (OMB) FISMA and information technology (IT) security guidance; and information on reported security incidents. We conducted our work, in support of this testimony, during February 2008 in the Washington, D.C. area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Over the past several years, agencies have consistently reported progress in performing certain information security control activities. According to the President's proposed fiscal year 2009 budget for information technology, the federal government continued to improve information security performance in fiscal year 2007 relative to key performance metrics established by OMB. The percentage of certified and accredited systems governmentwide reportedly increased from 88 percent to 92 percent.[4] Gains were also reported in testing of security controls – from 88 percent of systems to 95 percent of systems – and for contingency plan testing – from 77 percent to 86 percent. These gains continue a historical trend that

[3]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.

[4]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.

we reported on last year.[5] At that time, agency IGs identified weaknesses in the processes several agencies use to implement these and other security program activities.

Despite the reported progress, federal agencies continue to confront long-standing information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always effectively manage the configuration of network devices to prevent unauthorized access and ensure system integrity, install patches on key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Nevertheless, there are opportunities for federal agencies to bolster information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For example, OMB has established an information system security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and

[5]GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

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. Therefore, it is important for agencies to safeguard their systems against risks such as loss or theft of resources (such as federal payments and collections), modification or destruction of data, and unauthorized uses of computer resources 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 or agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Critical Systems Face Multiple Cyber Threats

Cyber threats to federal systems and critical infrastructures can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual specifically attacks a critical infrastructure system. A nontargeted attack occurs when the intended target of the attack is uncertain,

such as when a virus, worm, or malware[6] is released on the Internet with no specific target. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical information systems, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of cyber threats to our nation's information systems and infrastructures.

[6]"Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

Table 1: Sources of Cyber Threats to Federal Systems and Critical Infrastructures

Threat source	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Foreign nation states	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. Also, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of the Central Intelligence Agency, can affect the daily lives of Americans across the country.[a]
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa macro virus, the Explore.Zip worm, the CIH (Chernobyl) virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a]Prepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack. According to the Director of National Intelligence,[7] "Our information infrastructure—including the internet, telecommunications

[7]*Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence*, Feb. 5, 2008.

networks, computer systems, and embedded processors and controllers in critical industries—increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year."

Increased Vulnerabilities Could Expose Federal Systems to Attack

As federal information systems increase their connectivity with other networks and the Internet and as the system capabilities continue to increase, federal systems will become increasingly more vulnerable. Data from the National Vulnerability Database, the U.S. government repository of standards-based vulnerability management data, showed that, as of February 6, 2008, there were about 29,000 security vulnerabilities or software defects that can be directly used by a hacker to gain access to a system or network. On average, close to 17 new vulnerabilities are added each day. Furthermore, the database revealed that more than 13,000 products contained security vulnerabilities.

These vulnerabilities become particularly significant when considering the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. Thus, protecting federal computer systems and the systems that support critical infrastructures has never been more important.

Federal Law and Policy Established Federal Information Security Requirements

Over five years have passed since Congress enacted FISMA, which sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA's framework creates a cycle of risk management activities necessary for an effective security program, and these activities are similar to 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 control effectiveness. More specifically, FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems used or operated by the agency or on behalf of the agency. In this regard, FISMA requires that agencies implement information security programs that, among other things, include

- periodic assessments of the risk;
- risk-based policies and procedures;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations.

[8]GAO, *Executive Guide: Information Security Management Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May, 1998).

In addition, agencies must develop and maintain an inventory of major information systems that is updated at least annually and report annually to the Director of OMB and several Congressional Committees on the adequacy and effectiveness of their information security policies, procedures, and practices and compliance with the requirements of the act.

OMB and agency IGs also play key roles under FISMA. Among other responsibilities, OMB is to develop policies, principles, standards, and guidelines on information security and is required to report annually to Congress on agency compliance with the requirements of the act. OMB has provided instructions to federal agencies and their IGs for annual FISMA reporting. OMB's reporting instructions focus on performance metrics related to the performance of key control activities such as certifying and accrediting systems, testing and evaluating security controls, and providing security training to personnel. Its yearly guidance also requires agencies to identify any physical or electronic incidents involving the loss of, or unauthorized access to, personally identifiable information.

FISMA also requires agency IGs to perform an independent evaluation of the information security programs and practices of the agency to determine the effectiveness of such programs and practices. Each evaluation is to include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assessing compliance (based on the results of the testing) with FISMA requirements and related information security policies, procedures, standards, and guidelines. These required evaluations are then submitted by each agency to OMB in the form of an OMB-developed template that summarizes the results. In addition to the template submission, OMB encourages agency IGs to provide any additional narrative in an appendix to the report to the extent they provide meaningful insight into the status of the agency's security or privacy program.

Agencies Report Progress in Performing Control Activities

Federal agencies continue to report progress in implementing key information security activities. The President's proposed fiscal year 2009 budget for IT states that the federal government continues to improve information security performance relative to the certification and accreditation of systems and the testing of security controls and contingency plans. According to the budget, in 2007 the percentage of certified and accredited systems rose from 88 percent to 92 percent. Even greater gains were reported in testing of security controls—from 88 percent of systems to 95 percent of systems—and for contingency plan testing—from 77 percent to 86 percent.

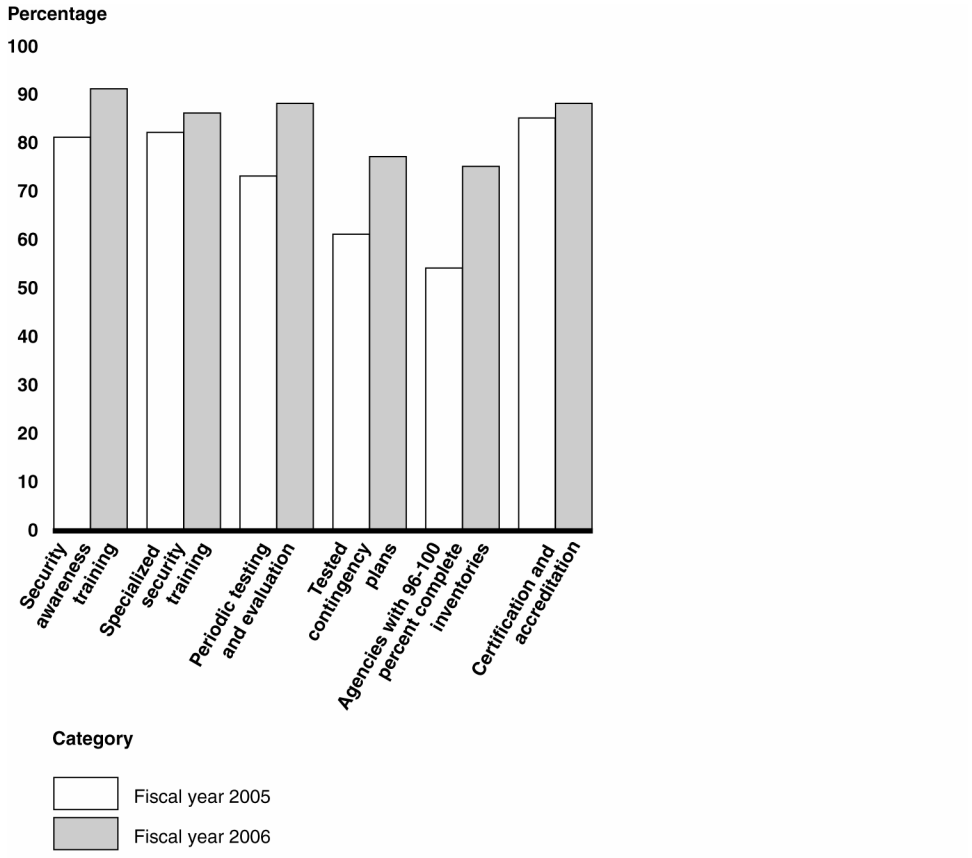
The proposed budget also noted improvements related to agency IG qualitative assessments of certain IT security processes. It reported that the overall quality of the certification and accreditation processes as determined by agency IGs increased compared to 2006, with 76 percent of agencies reporting "satisfactory" or better processes, up from 60 percent the prior year. In addition, the budget noted that 76 percent of agencies demonstrated that they had an effective process in place for identifying and correcting weaknesses using Plans of Action and Milestone management processes.

Although we have not yet verified the information security performance information for fiscal year 2007 contained in the President's proposed budget, the information is consistent with historical trends. As we reported last year, agencies reported increased percentages in most OMB performance metrics for fiscal year 2006 when compared to fiscal year 2005 (see fig. 1) including those related to:

- Percentage of employees and contractors receiving IT security awareness training,
- Percentage of employees with significant security responsibilities who received specialized security training,
- Percentage of systems whose controls were tested and evaluated,

- Percentage of systems with tested contingency plans,
- Percentage of 24 major agencies with 96-100 percent complete inventories of major information systems, and
- Percentage of systems certified and accredited.

Figure 1: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of agency FISMA reports.

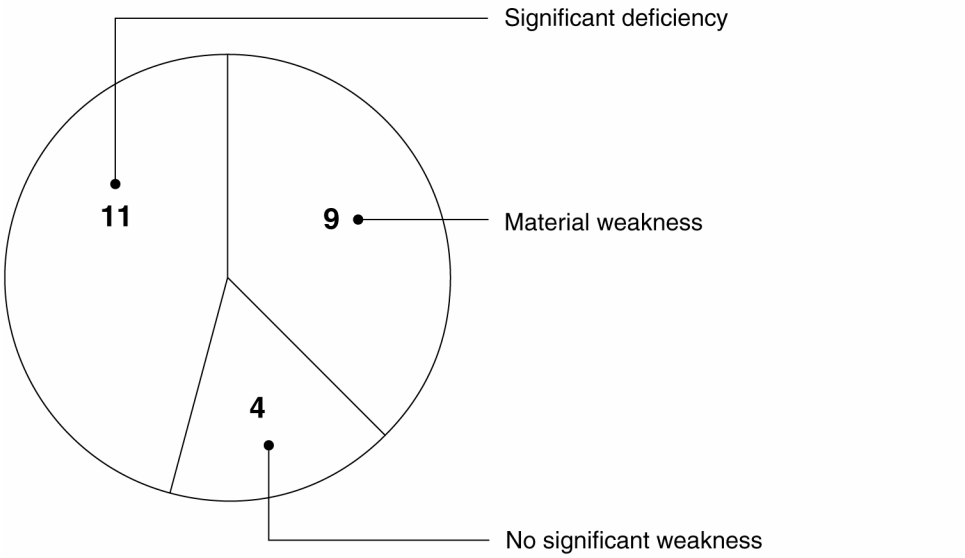
However, for the fiscal year 2006 reporting period, IGs identified weaknesses with their agencies' implementations of those key control activities. For example, according to agency IGs, five major agencies reported challenges in ensuring that contractors had received security awareness training. In addition, they reported that not all systems had been tested and evaluated at least annually, including some high impact systems, and that weaknesses existed in agencies' monitoring of contractor systems or facilities. They highlighted other weaknesses such as contingency plans not being completed for critical systems and inventories of systems that were incomplete. Furthermore, IGs reported weaknesses in agencies' certification and accreditation processes, a key activity OMB uses to monitor agencies' implementation of information security requirements.

Despite Reported Progress, Significant Control Deficiencies Persist at Federal Agencies

Our work and that of IGs show that significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. In their fiscal year 2007 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information security controls were either a significant deficiency or a material weakness (see fig. 2).[9] Our audits continue to identify similar conditions in both financial and non-financial systems, including agencywide weaknesses as well as weaknesses in critical federal systems.

[9]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.

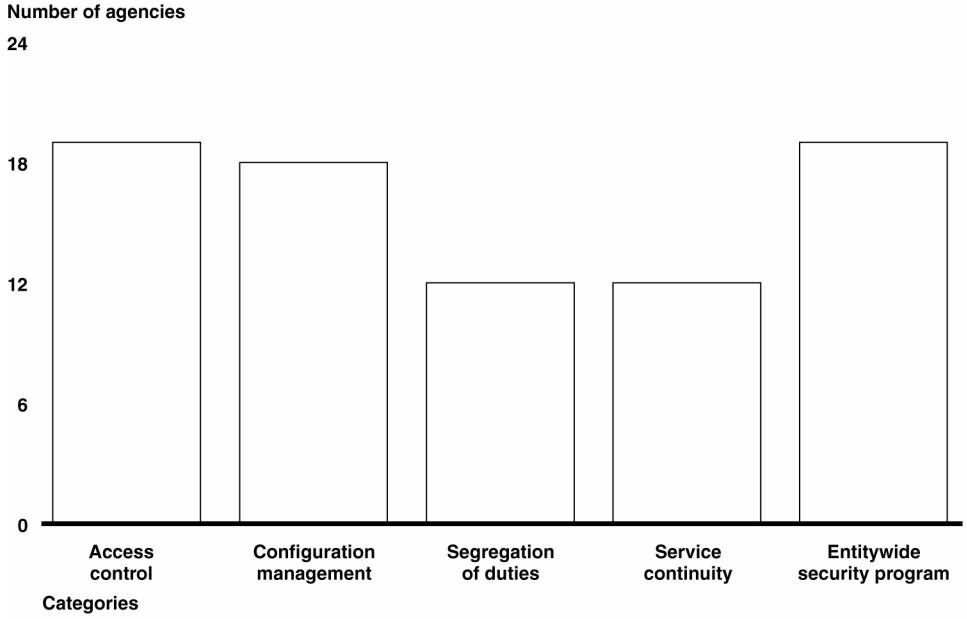
Figure 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2007.

Persistent weaknesses appear in 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 3 shows the number of major agencies with weaknesses in these five areas.

Figure 3: Number of Major Agencies Reporting Weaknesses in Control Categories



Source: GAO analysis of agency performance and accountability reports for FY2007.

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.

Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. To illustrate, 19 of 24 major agencies reported weaknesses in such controls. For example,

agencies did not consistently (1) identify and authenticate users to prevent unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. Agencies also lacked effective controls to restrict physical access to information assets. We previously reported that many of the data losses occurring 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.

Weaknesses Also 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 the policies, procedures, and techniques for ensuring that computer hardware and software are configured in accordance with agency policies and that software patches are installed in a timely manner; appropriately segregating incompatible duties; and establishing plans and procedures to ensure continuity of operations for systems that support the operations and assets of the agency.

However, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, agencies did not always ensure that continuity of operations plans contained all essential information. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented all the FISMA-required elements for an agencywide information security program. An agencywide security program,

required by FISMA, provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that 19 of 24 major federal agencies had not fully implemented agencywide information security programs. Our recent reports illustrate that agencies often did not adequately design or effectively implement policies for elements key to an information security program.

We identified weaknesses in information security program activities, such as agencies' risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. For example,

- One agency's risk assessment was completed without the benefit of an inventory of all the interconnections between it and other systems. In another case, an agency had assessed and categorized system risk levels and conducted risk assessments, but did not identify many of the vulnerabilities we found and had not subsequently assessed the risks associated with them.
- Agencies had developed and documented information security policies, standards, and guidelines for information security, but did not always provide specific guidance for securing critical systems or implement guidance concerning systems that processed Privacy Act-protected data.
- Security plans were not always up-to-date or complete.
- Agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.
- Agencies had tested and evaluated information security controls, but their testing was not always comprehensive and did not identify many of the vulnerabilities we identified.

- Agencies did not consistently document weaknesses or resources in remedial action plans.

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, and responsibilities may be unclear, misunderstood, and improperly implemented. 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. Consequently, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. In prior reports, we and the IGs have made hundreds of recommendations to agencies to address specific information security control weaknesses and program shortfalls. Until agencies effectively and fully implement agencywide information security programs, including addressing the hundreds of recommendations that we and IGs have made, federal information and information systems will not be adequately safeguarded to prevent their disruption, unauthorized use, disclosure, or modification.

Incidents at Federal Agencies Place Sensitive Information and Systems at Risk

The need for effective information security policies and practices is further illustrated by the number of security incidents experienced by federal agencies that put sensitive information at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

These incidents illustrate that a broad array of federal information and critical infrastructures are at risk.

- The Department of Veterans Affairs (VA) announced that computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Until the equipment was recovered, veterans did not know whether their information was likely to be misused. In June, VA sent notices to the affected individuals that explained the breach and offered advice concerning steps to reduce the risk of identity theft. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised.

- The Transportation Security Administration (TSA) announced a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005. An external hard drive containing personnel data, such as Social Security number, date of birth, payroll information, and bank account and routing information, was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital.

- A contractor for the Centers for Medicare and Medicaid Services reported the theft of one of its employee's laptop computer from his office. The computer contained personal information including names, telephone numbers, medical record numbers, and dates of birth of 49,572 Medicare beneficiaries.

- The Census Bureau reported 672 missing laptops, of which 246 contained some degree of personal data. Of the missing laptops containing personal information, almost half (104) were stolen, often from employees' vehicles, and another 113 were not returned by former employees. The Commerce Department reported that employees had not been held accountable for not returning their laptops.

- The Department of State experienced a breach on its unclassified network, which daily processes about 750,000 e-mails and instant messages from more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. The breach involved an e-mail containing what was thought to be an innocuous attachment.

However, the e-mail contained code to exploit vulnerabilities in a well-known application for which no security patch existed. Because the vendor was unable to expedite testing and deploy a new patch, the department developed its own temporary fix to protect systems from being further exploited. In addition, the department sanitized the infected computers and servers, rebuilt them, changed all passwords, installed critical patches, and updated their anti-virus software.

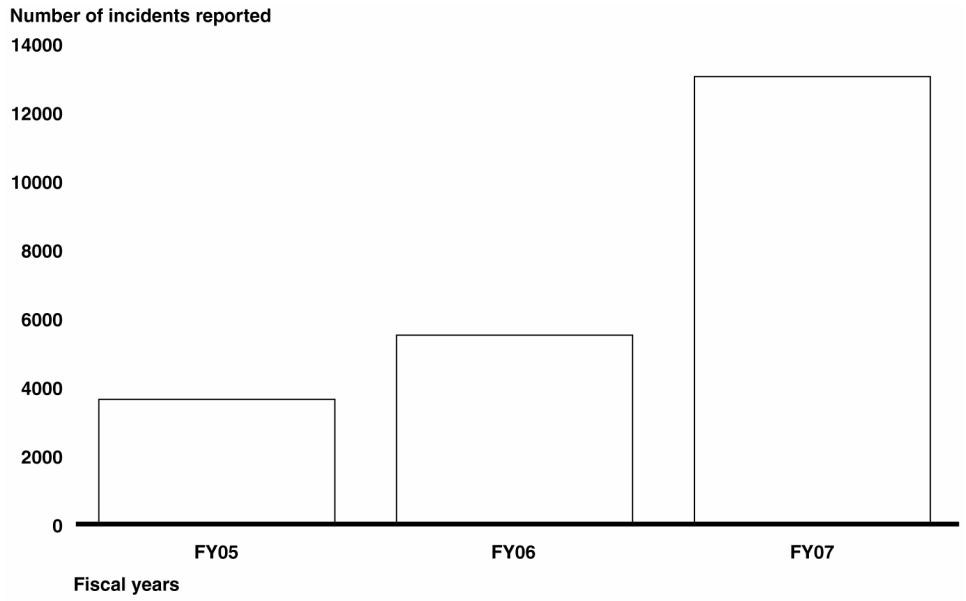
- In August 2006, two circulation pumps at Unit 3 of the Tennessee Valley Authority's Browns Ferry nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

- Officials at the Department of Commerce's Bureau of Industry and Security discovered a security breach in July 2006. In investigating this incident, officials were able to review firewall logs for an 8-month period prior to the initial detection of the incident, but were unable to clearly define the amount of time that perpetrators were inside its computers, or find any evidence to show that data was lost as a result.

- The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as "Slammer" infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.

When incidents such as these occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 4, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 3,634 incidents reported in fiscal year 2005 to 13,029 incidents in fiscal year 2007, (about a 259 percent increase).

Figure 4: Incidents Reported to US-CERT in Fiscal Years 2005 through 2007



Source: GAO analysis of US-CERT data.

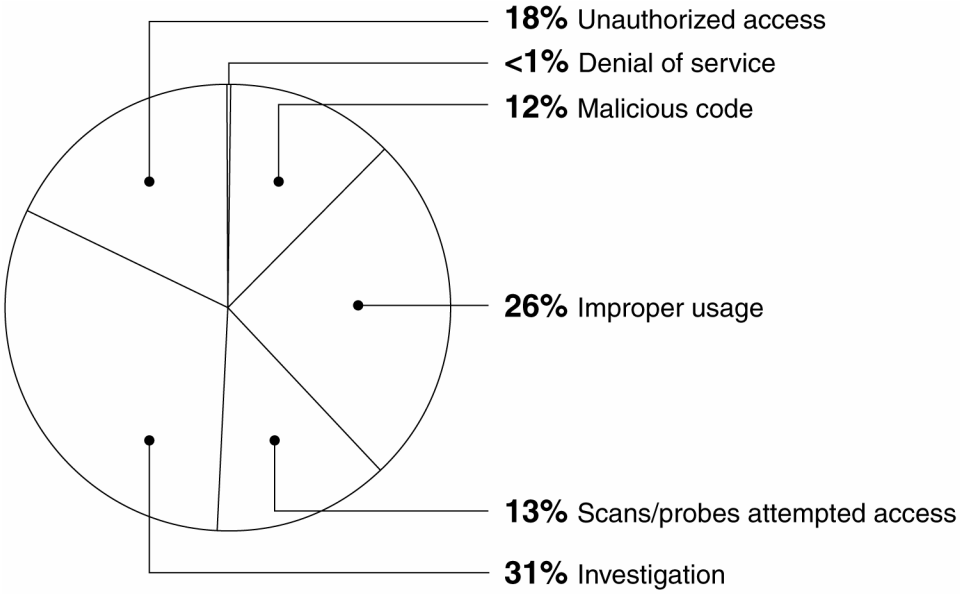
Incidents are categorized by US-CERT in the following manner:

- Unauthorized access: In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- Denial of service: An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in a denial of service attack.
- Malicious code: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
- Improper usage: A person violates acceptable computing use policies.

- Scans/probes/attempted access: This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.
- Investigation: Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 5, the three most prevalent types of incidents reported to US CERT in fiscal year 2007 were unauthorized access, improper usage, and investigation.

Figure 5. Percentage of Incidents Reported to US-CERT in FY07



Source: GAO analysis of US-CERT data.

Opportunities Exist for Enhancing Federal Information Security

In prior reports, GAO and IGs have made hundreds of recommendations to agencies for actions necessary to resolve prior

significant control deficiencies and information security program shortfalls. For example, we recommended agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring and physical security. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, recognizing the need for common solutions to improving security, OMB and certain federal agencies have continued or launched several government wide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *The Information Systems Security Line of Business*: The goal of this initiative is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.

- *Federal Desktop Core Configuration:* This initiative directs agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations develop by NIST, DOD, and DHS. The goal of this initiative is to improve information security and reduce overall IT operating costs.

- *SmartBUY:* This program, led by GSA, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.

- *Trusted Internet Connections initiative:* This is an effort designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of fifty.

  In addition to these initiatives, OMB has issued several policy memorandums over the past two years to help agencies protect sensitive data. For example, it has sent memorandums to agencies to reemphasize their responsibilities under law and policy to (1) appropriately safeguard sensitive and personally identifiable information, (2) train employees on their responsibilities to protect sensitive information, and (3) report security incidents. In May 2007, OMB issued additional detailed guidelines to agencies on safeguarding against and responding to the breach of personally identifiable information, including developing and implementing a risk-based breach notification policy, reviewing and reducing current holdings of personal information, protecting federal information accessed remotely, and developing and implementing a policy outlining the rules of behavior, as well as identifying consequences and potential corrective actions for failure to follow these rules.

  Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

- *Clarify requirements for testing and evaluating security controls.* Periodic testing and evaluation of information security controls is a critical element for ensuring that controls are properly designed, operating effectively, and achieving control objectives. FISMA requires that agency information security programs include the testing and evaluation of the effectiveness of information security policies, procedures, and practices, and that such tests be performed with a frequency depending on risk, but no less than annually.

We previously reported[10] that federal agencies had not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Agency policies often did not include important elements for performing effective testing such as how to determine the frequency, depth, and breadth of testing according to risk. In addition, the methods and practices for at six test case agencies were not adequate to ensure that assessments were consistent, of similar quality, or repeatable. For example, these agencies did not define the assessment methods to be used when evaluating security controls, did not test controls as prescribed, and did not include previously reported remedial actions or weaknesses in their test plans to ensure that they had been addressed. In addition, our audits of information security controls often identify weaknesses that agency or contractor personnel who tested the controls of the same systems did not identify. Clarifying or strengthening federal policies and requirements for determining the frequency, depth, and breadth of security controls according to risk could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations, and assets.

- *Enhance FISMA reporting requirements*. Periodic reporting of performance measures for FISMA requirements and related analyses provides valuable information on the status and progress of agency efforts to implement effective security management programs.

  In previous reports, we have recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting IGs to report on the quality of additional performance metrics. OMB has taken steps to enhance its reporting instructions. For example, OMB added questions regarding incident detection and assessments of system inventory. However, the current metrics do not measure how effectively agencies are performing various activities. Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, agencies are required to test and evaluate

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

the effectiveness of the controls over their systems at least once a year and to report on the number of systems undergoing such tests. However, there is no measure of the quality of agencies' test and evaluation processes. Similarly, OMB's reporting instructions do not address the quality of other activities such as risk categorization, security awareness training, intrusion detection and prevention, or incident reporting. OMB has recognized the need for assurance of quality for agency processes. For example, it specifically requested that the IGs evaluate the certification and accreditation process. The qualitative assessments of the process allows the IG to rate its agency's certification and accreditation process using the terms "excellent," "good," "satisfactory," "poor," or "failing." Providing information on the quality of the processes used to implement key control activities would further enhance the usefulness of the annually reported data for management and oversight purposes.

We also previously reported that OMB's reporting guidance and performance measures did not include complete reporting on certain key FISMA-related activities. For example, FISMA requires each agency to include policies and procedures in its security program that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In our report on patch management,[11] we stated that maintaining up-to-date patches is key to complying with this requirement. As such, we recommended that OMB address patch management in its FISMA reporting instructions. Although OMB addressed patch management in its 2004 FISMA reporting instructions, it no longer requests this information. As a result, OMB and the Congress lack information that could identify governmentwide issues regarding patch management. This information could prove useful in demonstrating whether or not agencies are taking appropriate steps for protecting their systems.

- *Consider conducting FISMA-mandated annual independent evaluations in accordance with audit standards or a common approach and framework.* We previously reported that the annual IG

[11]GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

FISMA evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies. For example:

- IGs stated that they were unable to conduct evaluations of their respective agency's inventory because the information provided to them by the agency at that time was insufficient (i.e. incomplete or unavailable).
- IGs reported interviewing officials and reviewing agency documentation, while others indicated conducting tests of implementation plans (e.g. security plans).
- IGs indicated in the scope and methodology sections of their reports that their reviews were focused on selected components, whereas others did not make any reference to the breadth of their review.
- Reports were solely comprised of a summary of relevant information security audits conducted during the fiscal year, while others included additional evaluation that addressed specific FISMA-required elements, such as risk assessments and remedial actions.
- The percentage of systems reviewed was varied. Twenty-two of 24 IGs tested the information security program effectiveness on a subset of systems; two IGs did not review any systems.
- One IG noted that the agency's inventory was missing certain web applications and concluded that the agency's inventory was only 0-50 percent complete, although the report also noted that, due to time constraints, the IG had been unable to determine whether other items were missing.
- Two IGs indicated basing a portion of their template submission solely on information provided to them by the agency, without conducting further investigation.

As we previously reported, the lack of a common methodology, or framework, had culminated in disparities in audit scope, methodology, and content of the IGs' annual independent

evaluations. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency. Conducting the evaluations in accordance with generally accepted government auditing standards and/or a commonly used framework or methodology could provide improved effectiveness, increased efficiency, quality control, and consistency in assessing whether the agency has an effective information security program. IGs may be able to use the framework to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently. Having a documented methodology may also offer quality control by providing a standardized methodology, which can help the IG community obtain consistency of application.

In summary, agencies have reported progress in implementing control activities, but persistent weaknesses in agency information security controls threaten the confidentiality, integrity, and availability of federal information and information systems, as illustrated by the increasing number of reported security incidents. Opportunities exist to improve information security at federal agencies. OMB and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation and FISMA reporting. Similarly, a consideration for strengthening the statutory requirement for the independent annual evaluations of agency information security programs required by FISMA could include requiring IGs to conduct the evaluation in accordance with generally accepted government auditing standards. Until such opportunities are seized and fully exploited and the hundreds of GAO and IG recommendations to mitigate information security control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain at undue and unnecessary risk.

Mr. Chairmen and Members of the Subcommittees, this concludes my statement. I would be happy to answer questions at this time.

Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Nancy DeFranceso (Assistant Director), Larry Crosland, Neil Doherty, Nancy Glover, Rebecca LaPaze, Stephanie Lee, and Jayne Wilson.