United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Government Management, Organization, and Procurement; House Committee on Oversight and Government Reform

For Release on Delivery
Expected at time 2:00 p.m. EDT
May 5, 2009

INFORMATION SECURITY

Cyber Threats and Vulnerabilities Place Federal Systems at Risk

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

May 5, 2009

INFORMATION SECURITY

Cyber Threats and Vulnerabilities Place Federal Systems at Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-661T, a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

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 maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

GAO was asked to describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. To do so, GAO relied on its previous reports and reviewed agency and inspectors general reports on information security.

What GAO Recommends

In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View GAO-09-661T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. These threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources, such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Moreover, these groups and individuals have a variety of attack techniques at their disposal, and cyber exploitation activity has grown more sophisticated, more targeted, and more serious. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. In the absence of robust security programs, 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 developments have led government officials to become increasingly concerned about the potential for a cyber attack.

According to GAO reports and annual security reporting, federal systems are not sufficiently protected to consistently thwart cyber threats. Serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. For example, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, and information, and weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. Agencies also did not always configure network devices and service properly, segregate incompatible duties, or ensure that continuity of operations plans contained all essential information. An underlying cause for these weaknesses is that agencies have not yet fully or effectively implemented key elements of their agencywide information security programs. To improve information security, efforts have been initiated that are intended to strengthen the protection of federal information and information systems. For example, the Comprehensive National Cybersecurity Initiative was launched in January 2008 and is intended to improve federal efforts to protect against intrusion attempts and anticipate future threats. Until such opportunities are seized and fully exploited and GAO recommendations to mitigate identified control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain vulnerable.

Chairwoman Watson and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on the threats, vulnerabilities, and challenges in securing federal information 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 maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

In my testimony today, I will describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. In preparing for this testimony, we relied on our previous reports on federal information security. These reports contain detailed overviews of the scope and methodology we used. We also reviewed inspectors general (IG) reports on information security, analyzed performance and accountability reports for 24 major federal agencies,[1] and examined information provided by the U.S. Computer Emergency Readiness Team (US-CERT) on reported security incidents.

We conducted our work in support of this testimony during April and May 2009, in the Washington, D.C. area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

[1] 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.

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. 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, deliver services to the public, and account for their resources without these information assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their information and information systems. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets. For example:

- Resources, such as federal payments and collections, could be lost or stolen.
- 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, intellectual property, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities.

Federal Systems and Infrastructures Face Increasing Cyber Threats

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. In September 2007, we reported[2] that these threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures, and equipment failures that inadvertently disrupt systems or corrupt data. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual attacks a specific system or cyber-based critical infrastructure. A nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or other malicious software[3] is released on the Internet with no specific target.

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.[4] The Federal Bureau of Investigation has identified multiple sources of threats to our

[2]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

[3]"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.

[4]Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

nation's critical information systems, including foreign nations engaged in espionage and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees and contractors 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 cyber infrastructures.

Table 1: Sources of Cyber Threats

Threat source	Description
Foreign nations	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, a growing array of state and nonstate adversaries are increasingly targeting—for exploitation and potentially disruption or destruction—information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.[a]
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
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.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a] Prepared statement of Dennis Blair, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 12, 2009.

These groups and individuals have a variety of attack techniques at their disposal. Furthermore, as we have previously reported,[5] the

[5]GAO, *Cybercrime: Public and Private Entities Face Challenges is Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

techniques have characteristics that can vastly enhance the reach and impact of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple state and national borders.
- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Attackers can more easily remain anonymous.

Table 2 identifies the types and techniques of cyber attacks that are commonly used.[6]

Table 2: Types and Techniques of Cyber Attacks

Type of attack	Description
Denial of service	A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bomb	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering even occurs, such as terminating the programmer's employment.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected files is loaded into memory, allowing the virus to infect other files. Unlike the computer worms, a virus requires human involvement (usually unwitting) to propagate.

[6]GAO-07-705 and GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: May 28, 2004).

Type of attack	Description
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
War-dialing	Simple program that dial consecutive phone numbers looking for a modem.
War-driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be sued as a delivery mechanism for malicious software and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial information from the sea of internet users.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

Source: GAO.

Government officials are increasingly concerned about the potential for a cyber attack. According to the Director of National Intelligence,[7] the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical infrastructures. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of IT have moved overseas, the threat will continue to grow. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. For example, the Director of National Intelligence also stated that, in August 2008, the Georgian national government's Web sites were disabled during hostilities with Russia, which hindered the government's ability to

[7]Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

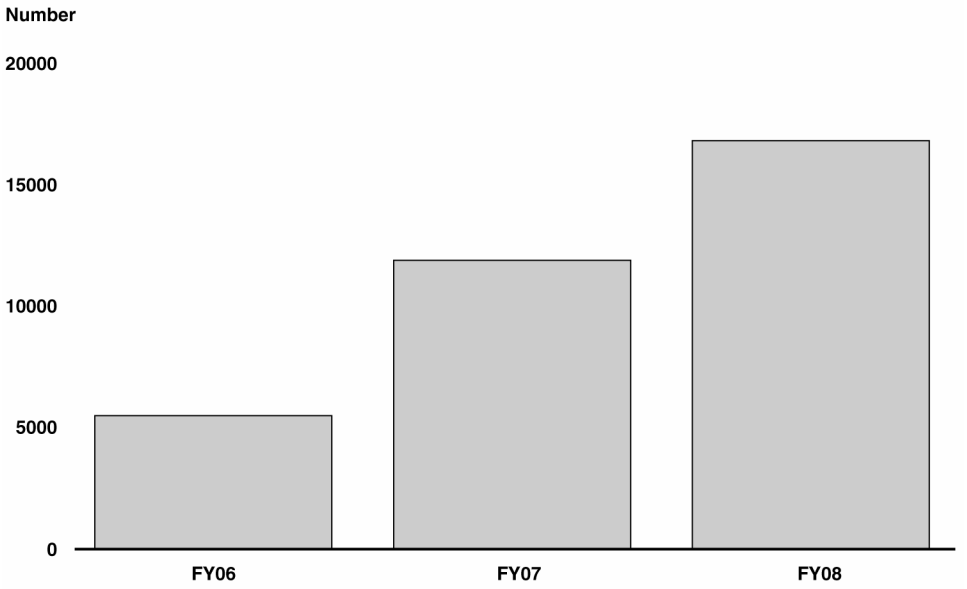
communicate its perspective about the conflict. The director expects disruptive cyber activities to become the norm in future political and military conflicts.

Reported Security Incidents Are on the Rise

Perhaps reflective of the evolving and growing nature of the threats to federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about 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.

When incidents occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (about a 206 percent increase).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2006 through 2008



Source: GAO analysis of US-CERT data.

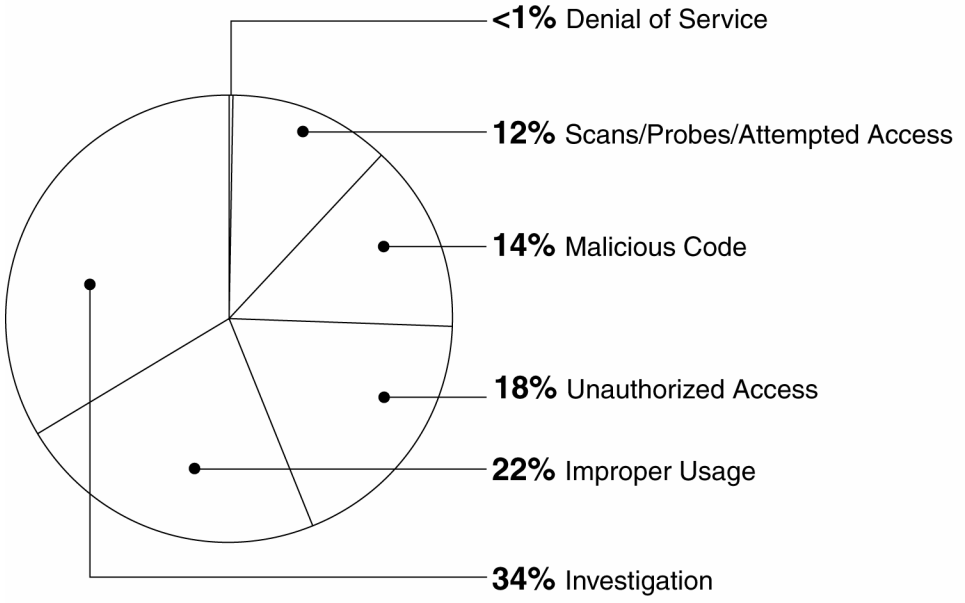
Incidents are categorized by US-CERT in the following manner:

- 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 2, the three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access, improper usage, and investigation.

Figure 2: Percentage of Incidents Reported to US-CERT in FY06-FY08 by Category



Source: GAO analysis of US-CERT data.

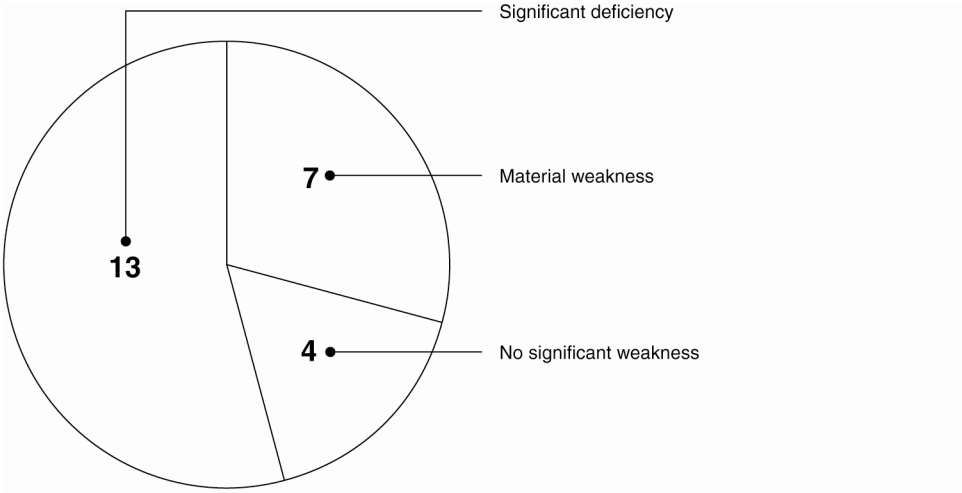
Vulnerabilities Pervade Federal Information Systems

The growing threats and increasing number of reported incidents, highlight the need for effective information security policies and practices. However, serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information system controls over financial systems and information were either a significant deficiency or a material weakness for financial statement reporting (see fig. 3).[8]

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

Figure 3: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2008.

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example:

- We reported in September 2008[9] that although the Los Alamos National Laboratory (LANL)—one of the nation's weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources. As a result, sensitive information on the network—including unclassified controlled nuclear information, naval nuclear propulsion information, export control information, and personally identifiable information—were exposed to an

[9] GAO, *Information Security: Actions Needed to Better Protect Lost Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

unnecessary risk of compromise. Moreover, the risk was heightened because about 300 (or 44 percent) of 688 foreign nationals who had access to the unclassified network as of May 2008 were from countries classified as sensitive by the Department of Energy, such as China, India, and Russia.

- In May 2008[10] we reported that the Tennessee Valley Authority (TVA)— a federal corporation and the nation's largest public power company that generates and transmits electricity using its 52 fossil, hydro, and nuclear power plants and transmission facilities—had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures. Both its corporate network infrastructure and control systems networks and devices at individual facilities and plants were vulnerable to disruption. In addition, the interconnections between TVA's control system networks and its corporate network increased the risk that security weaknesses, on the corporate network could affect control systems networks and we determined that the control systems were at increased risk of unauthorized modification or disruption by both internal and external threats. These deficiencies placed TVA at increased and unnecessary risk of being unable to respond properly to a major disruption resulting from an intended or unintended cyber incident, which could then, in turn, affect the agency's operations and its customers.

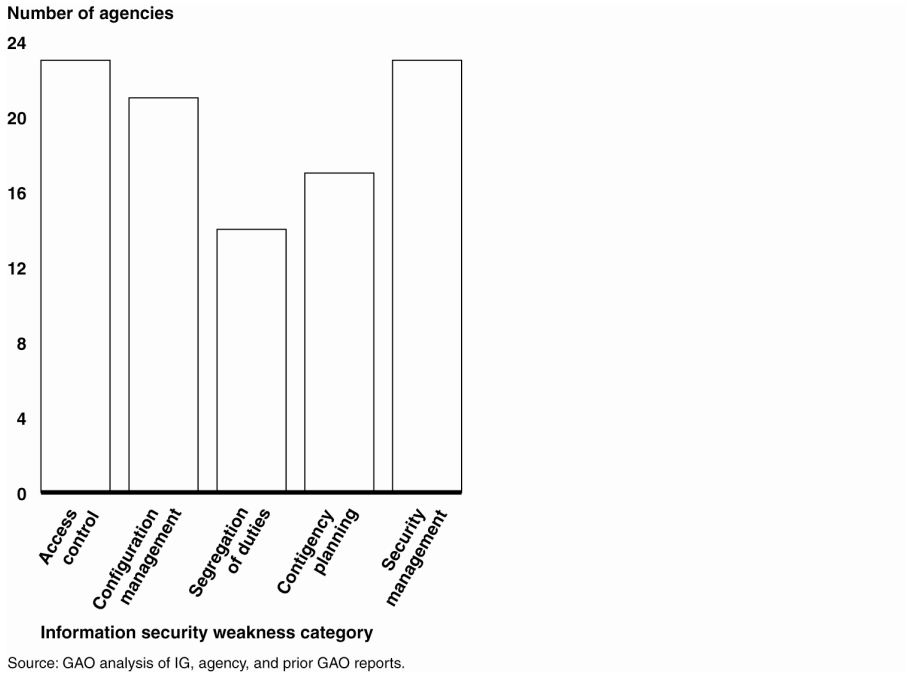
Weaknesses Persist in All Major Categories of Controls

Vulnerabilities in the form of inadequate information system controls have been found repeatedly in our prior reports as well as IG and agency reports. These weaknesses fall into 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 security features for hardware and software are identified and implemented and that changes to that configuration are systematically controlled; (3) segregation of duties, which

[10] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

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 4 shows the number of major agencies with weaknesses in these five areas.

Figure 4: Number of Major Agencies Reporting Weaknesses by Control Category for Fiscal Year 2008



Source: GAO analysis of IG, agency, and prior GAO reports.

Over the last several years, most agencies have not implemented 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, weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. 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. At least nine 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.

In addition, 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 necessary to restore services in a timely manner. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program. An agencywide security program, required by the Federal Information Security Management Act[11], 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 23 of 24 major federal agencies had weaknesses in their agencywide information security programs.

[11] *Federal Information Security Management Act of 2002,* Title III*, E-Government Act of 2002,* Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

Due to the persistent nature of these vulnerabilities and associated risks, we continued to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress;[12] a designation we have made in each report since 1997.

Opportunities Exist for Enhancing Federal Information Security

Over the past several years, we and the 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 that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting shortcomings 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, the White House, the Office of Management and Budget (OMB), and certain federal agencies have continued or launched several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *Comprehensive National Cybersecurity Initiative*: In January 2008, President Bush began to implement a series of initiatives aimed primarily at improving the Department of Homeland Security and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[13] While these initiatives have not been made public, the Director of National Intelligence stated that they

[12]GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

[13]The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.[14]

- *The Information Systems Security Line of Business*: The goal of this initiative, led by OMB, 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*: For this initiative, OMB directed agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by the National Institute of Standards and Technology, Department of Defense, and Department of Homeland Security. The goal of this initiative is to improve information security and reduce overall IT operating costs.

- *SmartBUY*: This program, led by the General Services Administration, 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 50.

[14]Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

In summary, the threats to federal information systems are evolving and growing, and federal systems are not sufficiently protected to consistently thwart the threats. Unintended incidents and attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations, have the potential to cause significant damage to the ability of agencies to effectively perform their missions, deliver services to constituents, and account for their resources. Opportunities exist to improve information security at federal agencies. The White House, OMB, and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. Until such opportunities are seized and fully exploited, and agencies fully and effectively implement the hundreds of recommendations by us and by IGs to mitigate information security control deficiencies and implement agencywide information security programs, federal information and systems will remain vulnerable.

Chairwoman Watson, this concludes my statement. I would be happy to answer questions at the appropriate 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 Charles Vrabel (Assistant Director), Larry Crosland, Neil Doherty, Rebecca LaPaze, and Jayne Wilson.