United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, March 24, 2010

INFORMATION SECURITY

Concerted Response Needed to Resolve Persistent Weaknesses

Statement of Gregory C. Wilshusen
Director, Information Security Issues

March 24, 2010

INFORMATION SECURITY

Concerted Response Needed to Resolve Persistent Weaknesses

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-536T, a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives

Why GAO Did This Study

Without proper safeguards, federal computer systems are vulnerable to intrusions by individuals who have malicious intentions and can obtain sensitive information. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained cyber attacks against the United States; these attacks continue to pose a potentially devastating impact to systems as well as the operations and critical infrastructures that they support. Concerned by reports of weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on federal information security and agency efforts to comply with FISMA. This testimony summarizes (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. To prepare for this testimony, GAO analyzed its prior reports and those from 24 major federal agencies, their inspectors general, and the Office of Management and Budget (OMB).

What GAO Recommends

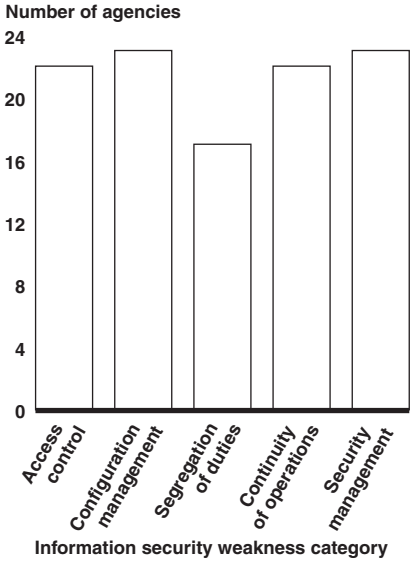
In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View GAO-10-536T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies have reported mixed progress in securing their systems and implementing key security activities. For example, in fiscal year 2009, agencies collectively reported an increasing percentage of personnel receiving security awareness training and specialized security training, but a decreasing rate of implementation for other key activities when compared to fiscal year 2008. In addition, federal systems continued to be afflicted by persistent control weaknesses. Almost all of the 24 major federal agencies had information security weaknesses in five key control categories, as illustrated in the figure below.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2009



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

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required by FISMA. As a result, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Opportunities exist to enhance federal cybersecurity through a concerted response to safeguarding systems that include several components. First, agencies can implement the hundreds of recommendations GAO and inspectors general have made to resolve control deficiencies and information security program shortfalls. In addition, OMB's continued efforts to improve reporting and oversight as recommended by GAO could help assess agency programs. Finally, the White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.

Chairwoman Watson and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on federal information security. As the number of reported computer security incidents and threats to the nation's cyber infrastructure steadily increase, the need for a vigilant and comprehensive approach to federal information security is greater than ever. In 2009, the federal government faced coordinated attacks against its Web sites, and several agencies were affected by the Gumblar Trojan, which uses multiple exploits to compromise legitimate web pages. In addition, the Conficker worm posed a threat to both federal and non-federal systems. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

Proper safeguards can mitigate the risk to federal computer systems and networks posed by individuals and groups with malicious intentions. While progress has been made in identifying and implementing these controls, much work remains. 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 the loss of privacy, identity theft, and other financial crimes.

In my testimony today, I will discuss (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. In conducting our review, we analyzed agency, inspector general, Office of Management and Budget (OMB), and our reports on information security. We conducted the review from December 2009 to March 2010 in the Washington, D.C., area in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

To help protect against threats to federal systems, the Federal Information Security Management Act (FISMA)[1] is intended to set forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Its framework creates a cycle of risk management activities necessary for an effective security program; these activities are similar to the principles noted in our study of the risk management activities of leading private sector organizations[2]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness.

In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to (1) agency heads and chief information officers, to develop, document, and implement an agencywide information security program, among other things; (2) inspectors general, to conduct annual independent evaluations of agency efforts to effectively implement information security; (3) the National Institute for Science and Technology (NIST), to provide standards and guidance to agencies on information security; and (4) OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing, at least annually, and approving or disapproving, agency information security programs. In addition, the act requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements. FISMA also requires OMB to report annually to Congress by March 1.

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

Although Agencies Report Mixed Progress, Deficiencies in Information Security Controls Remain

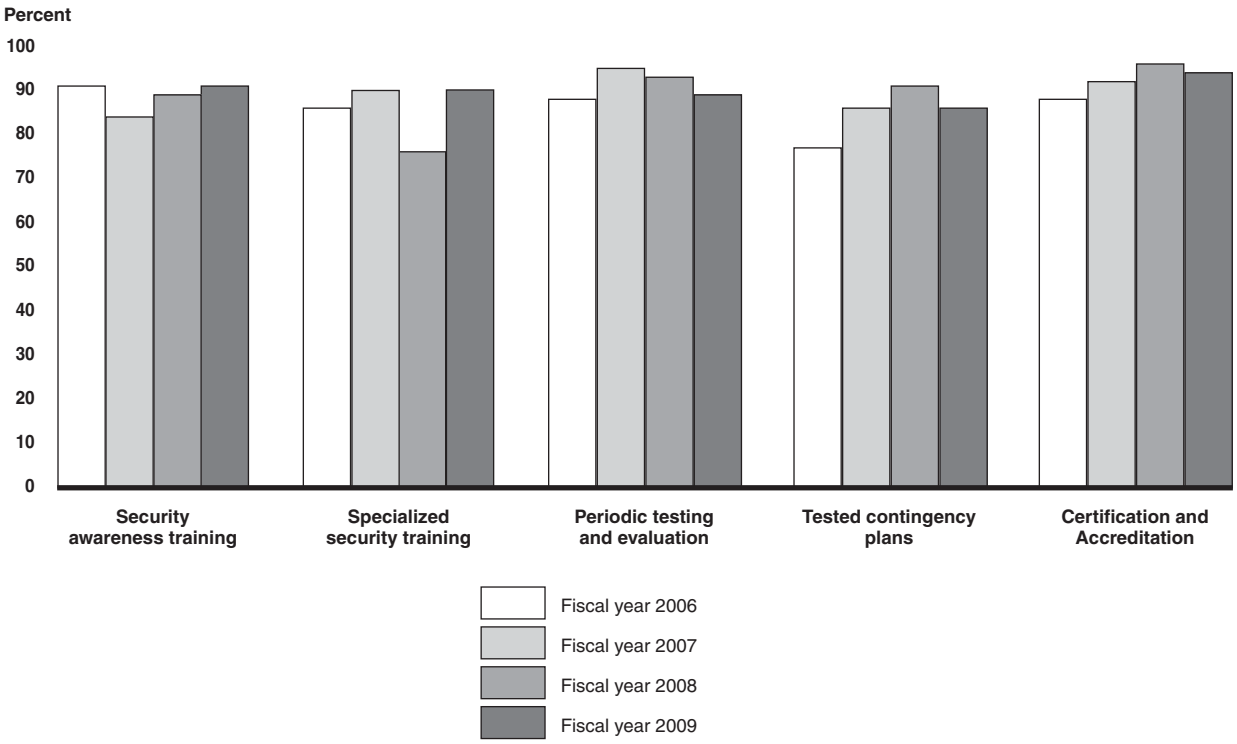
FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As part of its oversight responsibilities OMB requires agencies to report on specific performance measures, including:

- 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, and
- Percentage of systems certified and accredited.

Since the enactment of FISMA in 2002, federal agencies have generally reported increasing rates of implementation for key information security activities. However, in fiscal year 2009, agencies reported mixed progress in implementing these activities compared to fiscal year 2008. For example, governmentwide, agencies collectively reported that 91 percent of employees and contractors had received security awareness training in fiscal year 2009, up from 89 percent in fiscal year 2008. Agencies also reported that 90 percent of employees with significant information security responsibilities had received specialized training, up from 76 percent in fiscal year 2008.

In other key areas, agencies reported slight decreases from fiscal years 2008 to 2009. Specifically, the percentage of systems for which security controls have been tested and reviewed decreased from 93 percent to 89 percent, the percentage of systems with tested contingency plans decreased from 91 percent to 86 percent, and the percentage of systems certified and accredited decreased from 96 percent to 94 percent. A summary of these percentages is shown in figure 1.

Figure 1: Selected Performance Metrics for Agency Systems



Source: GAO analysis of agency data.

In these and other areas, inspectors general at the 24 major agencies have also reported weaknesses in their fiscal year 2009 audits and evaluations. Weaknesses in requirements such as periodic testing and evaluation, certification and accreditation, configuration management, and remedial actions were most commonly reported. For example,

- at least 13 inspectors general reported that their agencies had insecure configuration settings, or had not applied needed patches in a timely manner, or both;
- at least 15 inspectors general reported that their agency did not adequately assess security controls such as those recommended by NIST;
- at least 11 inspectors general reported that their agencies failed to create a remediation plan for all identified weaknesses.
- at least 13 inspectors general reported that documents required to make an informed decision regarding certification and accreditation of systems

were either missing or incomplete, or that the accreditation was allowed to expire on at least one system without recertification;

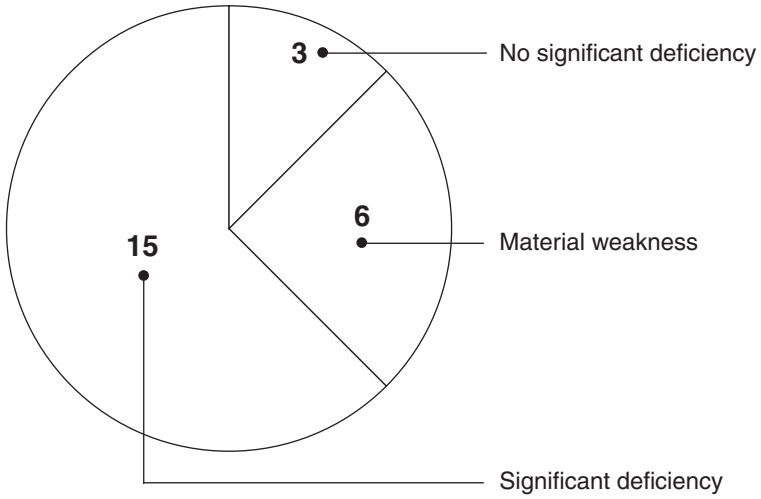
Weaknesses such as these continue to impair the government's ability to ensure the confidentiality, integrity, and availability of critical information and information systems used to support the operations and assets of federal agencies. Until these agencies fully implement information security requirements, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations.

Despite Reported Progress, Federal Systems Remain Vulnerable

GAO and agency inspectors general reviews continue to highlight deficiencies in the implementation of security policies and procedures at federal agencies. In their fiscal year 2009 performance and accountability reports, 21 of 24 major agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency (see fig. 2).[3]

[3]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 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security for Financial Reporting



Source: GAO analysis of agency performance and accountability report, annual financial report, or other financial statement reports for FY 2009.

Our audits and those of the inspectors general continue to identify similar conditions in both financial and non-financial systems. Most of the 24 major federal agencies had reported deficiencies in the following major categories of information security controls, as defined by our *Federal Information System Controls Audit Manual*:[4]

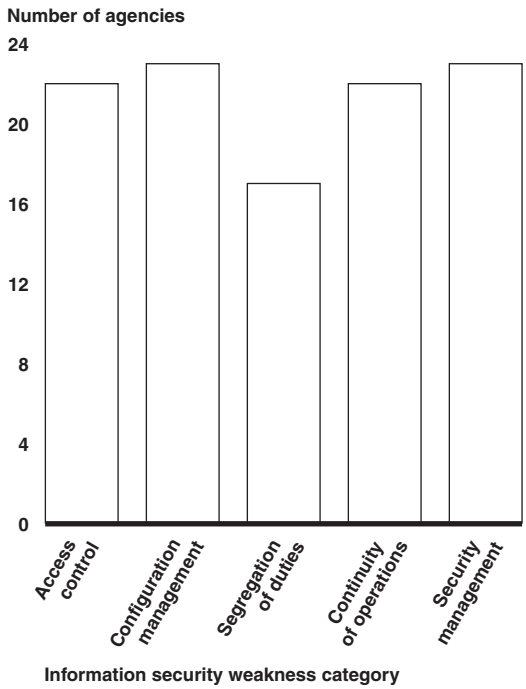
- access controls, which ensure that only authorized individuals can read, alter, or delete data;
- configuration management controls, which provide assurance that only authorized software programs are implemented;
- segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection;
- continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and

[4]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: Feb. 2009).

- an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

As shown in figure 3, agencies reported deficiencies in all five of the information security control areas. For example, agencies did not consistently configure network devices and services to prevent unauthorized access and ensure system integrity; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. Such information security control weaknesses unnecessarily increase the risk that the reliability and availability of data that are recorded in or transmitted by federal systems could be compromised.

Figure 3: Number of Major Agencies Reporting Weaknesses by Control Category for Fiscal Year 2009



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

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required

by FISMA. An agencywide security program provides a framework and continuing cycle of activity that includes 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. According to inspector general, agency, and our previous reports, 23 of the 24 major federal agencies had weaknesses in their agencywide information security programs.

The following examples, reported in 2009, illustrate that a broad array of federal information and systems remain at risk.

- At the Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, key information security program activities were not implemented.[5] For example, FinCEN did not always include detailed implementation guidance in its policies and procedures or adequately test and evaluate information security controls.

- The information security program for the classified computer network at the Los Alamos National Laboratory (LANL) had not been fully implemented.[6] Specifically, (1) risk assessments were not comprehensive, (2) specific guidance was missing from policies and procedures, (3) the training and awareness program did not adequately address specialized training needs for individuals with significant network security responsibilities, (4) system security plans were incomplete, (5) the system security testing and evaluation process had shortcomings, (6) corrective action plans were not comprehensive, and (7) contingency plans were incomplete and not tested. In addition, the laboratory's decentralized management approach has led to weaknesses in the effectiveness of its classified cybersecurity program. Although the laboratory has taken steps to address these weaknesses, its efforts may be limited because LANL has not demonstrated a consistent capacity to sustain security improvements over the long term.

[5]GAO, *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data*, GAO-09-195 (Washington, D.C.: Jan. 30, 2009).

[6]GAO, *Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network*, GAO-10-28 (Washington, D.C.: Oct. 14, 2009).

- We identified a number of shortcomings in key program activities at the National Aeronautics and Space Administration (NASA).[7] For example, NASA had not always (1) fully assessed information security risks; (2) fully developed and documented security policies and procedures; (3) included key information in security plans; (4) conducted comprehensive tests and evaluation of its information system controls; (5) tracked the status of plans to remedy known weaknesses; (6) planned for contingencies and disruptions in service; (7) maintained capabilities to detect, report, and respond to security incidents; and (8) incorporated important security requirements in its agreement with its contractor.

In addition, the inspectors general at 13 of the 24 major agencies reported information security as major management challenge. Due to the persistent nature of information security vulnerabilities and the associated risks, we continue to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress; a designation we have made in each report since 1997.[8]

Reported Security Incidents Are on the Rise

Consistent with the evolving and growing nature of the threats and persistent vulnerabilities to federal systems, agencies are reporting an increasing number of security incidents and events. 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.

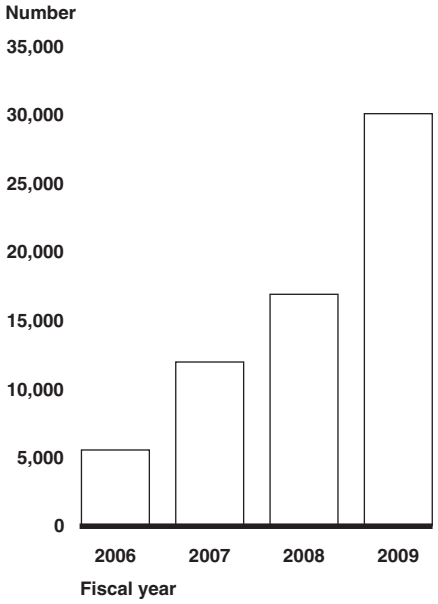
When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). US-CERT serves as a focal point for the government's interaction with federal and nonfederal entities on a 24-hour-a-day, 7-day-a-week basis regarding cyber-related analysis, warning,

[7]GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009).

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

information sharing, major incident response, and national-level recovery efforts. As shown in figure 4, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 4 years, increasing from 5,503 incidents reported in fiscal year 2006 to about 30,000 incidents in fiscal year 2009 (over a 400 percent increase).

Figure 4: Incidents Reported to US-CERT, FY 2006-2009



Source: GAO analysis of US-CERT data.

Agencies report the following types of incidents and events based on US-CERT-defined categories:

- **Unauthorized access:** Gaining logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- **Denial of service:** Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.
- **Malicious code:** Installing 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.

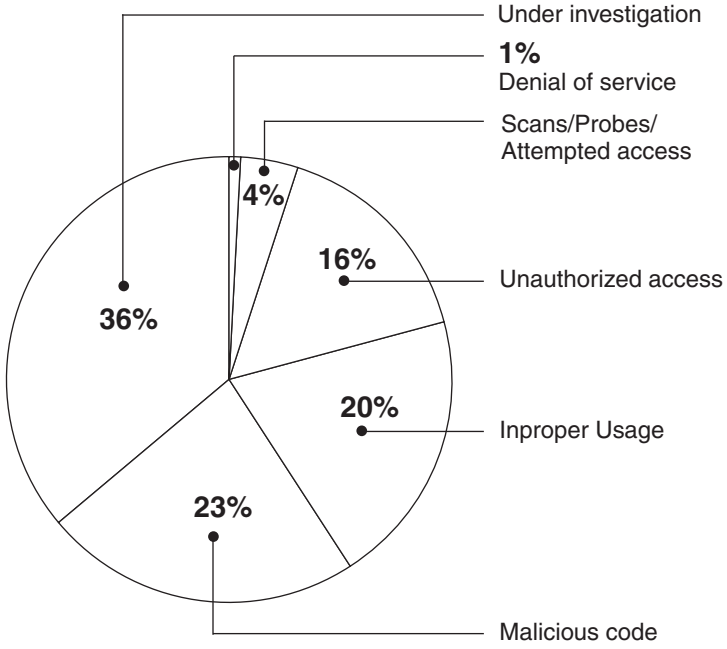
- **Improper usage:** Violating acceptable computing use policies.

- **Scans/probes/attempted access:** Accessing or identifying 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.

- **Unconfirmed incidents under investigation:** Investigating unconfirmed incidents that are potentially malicious, or anomalous activity deemed by the reporting entity to warrant further review.

The four most prevalent types of incidents and events reported to US-CERT during fiscal year 2009 were: (1) malicious code comprising 23 percent; (2) improper usage, 20 percent; (3) unauthorized access, 16 percent; and (4) unconfirmed incidents under investigation, 36 percent. Incidents reported to US-CERT in fiscal year 2009 are shown by type in figure 5.

Figure 5: Percentage of Incidents Reported to US-CERT in Fiscal Year 2009 by Category



Source: GAO analysis of U.S. CERT data.

Opportunities Exist for Enhancing Federal Cybersecurity

A concerted response to safeguarding federal systems includes several components. Agencies can take action to resolve specific security weaknesses, federal law and guidance can be strengthened, and continued effort can be made on governmentwide security initiatives.

Over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve significant control deficiencies and information security program shortfalls. Effective implementation of our recommendations will help agencies to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data. In addition, implementation of these recommendations will help agencies to better manage the configuration of security features for hardware and software and assure that changes to the configuration are systematically controlled.

We have also recommended that agencies fully implement comprehensive, agencywide information security programs, including by correcting weaknesses in specific areas of their programs such as: (1) assessments of the risk to information systems; (2) information security policies and procedures; (3) planning for interruptions to information system processing; (4) training personnel in awareness of security policies and procedures; (5) periodic tests and evaluations of the effectiveness of information system controls; and (6) the implementation of plans of action to remediate information security weaknesses. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

In addition, agencies can also increase their efficiency in securing and monitoring networks by expanding their use of automated tools as part of their monitoring programs for performing certain security-related functions. Because federal computing environments are very large, complex, and geographically dispersed, often consisting of tens or hundreds of thousands of devices, increasing automation of key security processes can assist in the efficient and effective implementation of key controls across the entire enterprise. For example, agencies can better use centrally administered automated diagnostic and analytical tools to continuously scan network traffic and devices across the enterprise to identify vulnerabilities or anomalies from typical usage and monitor compliance with agency configuration requirements. In addition, improving the use of automated tools for patch management can increase

efficiency in mitigating known vulnerabilities on many systems within an agency.

Strengthen FISMA and Its Implementing Guidance

FISMA was intended to provide (1) a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and (2) a mechanism for improved oversight of federal agency information security programs. In June 2009,[9] we proposed several suggested actions that could improve FISMA and its associated implementing guidance, including (1) clarifying requirements for testing and evaluating security controls; (2) requiring agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program; (3) enhancing independent annual evaluations; (4) strengthening annual reporting mechanisms; and (5) strengthening OMB oversight of agency information security programs. Implementing these suggestions can improve the implementation and oversight of federal agency information security programs.

Continue Efforts to Improve Reporting and Oversight

FISMA specifies that OMB is to develop policies, principles, standards, and guidelines on information security. Each year, OMB provides instructions to federal agencies and their inspectors general for preparing the annual FISMA reports. OMB developed an online reporting tool during fiscal year 2009 to improve the efficiency of the annual reporting process. Agencies are required to use the online tool to submit their annual reports and OMB is to use the data submitted in its online reporting tool to summarize the information provided by the agencies and the inspectors general in its report to Congress.

We have previously made several recommendations to OMB for improving its annual reporting instructions and oversight.[10] For example, we have recommended that OMB update its annual reporting instructions to request inspectors general report on the effectiveness of agencies'

[9]GAO, *Federal Information Security Issues*, GAO-09-817R (Washington, D.C.: June 30, 2009).

[10]GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, GAO-09-546 (Washington, D.C.: July 17, 2009) and *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

processes for developing inventories, monitoring contractor operations, and providing specialized security training. OMB has acted to enhance its reporting instructions; however, further actions need to be taken to fully address these recommendations.

We have also recommended that OMB develop metrics that (1) focus on the effectiveness of information security controls and (2) the overall impact of an agency's information security program.[11] In September 2009, OMB convened a Security Metrics Taskforce to develop new FISMA performance measures. According to OMB's website the taskforce is comprised of officials from the both the federal community and private sector and was tasked with developing metrics that focus on outcomes rather than compliance that agencies will be required to report as part of the FISMA reporting process. In December 2009, OMB released draft metrics for comment but has not yet released the final metrics.

Continue to Enhance Federal Information Security through Governmentwide Initiatives

The White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.

Address challenges in implementing CNCI. In January 2008, President Bush established the Comprehensive National Cybersecurity Initiative (CNCI). The initiative, which consists of 12 projects, is intended to reduce vulnerabilities, protect against intrusions, and anticipate future threats against federal executive branch information systems.[12] As we recently reported,[13] the White House and federal agencies have established interagency groups to plan and coordinate CNCI activities. However, CNCI faces challenges in achieving its objectives related to securing federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goals. Among other

[11]GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, GAO-09-617 (Washington, D.C.: Sep. 14, 2009).

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

[13]GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: March 5, 2010).

recommendations, we recommended that the Director of OMB take action to: (1) better define roles and responsibilities of all key CNCI participants; (2) establish measures to determine the effectiveness of CNCI projects in making federal information systems more secure and track progress against those measures; (3) establish an appropriate level of transparency about CNCI; and (4) reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems. OMB agreed with 3 of the 4 recommendations, disagreeing with the recommendation regarding defining roles and responsibilities. However, such definitions are key to achieving CNCI's objective of securing federal systems.

Continue efforts to implement TIC and Einstein initiatives. Two specific initiatives of CNCI are Trusted Internet Connections (TIC) and Einstein. TIC is an effort to consolidate the federal government's external access points (including those to the Internet). TIC is also intended to establish baseline security capabilities and validate agency adherence to those security capabilities. The Einstein initiative is a computer network intrusion detection system that analyzes network flow information from participating federal agencies. The system is to provide a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks. Einstein is intended to alert US-CERT in real time of this activity and provides correlation and visualization of the derived data. We have ongoing work that addresses status and implementation of these initiatives.

Continue efforts to implement FDCC. Under the Federal Desktop Core Configuration Initiative, OMB directed agencies that have Windows XP and/or Windows Vista operating systems deployed to adopt the security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs. We have ongoing work that addresses status and implementation of this initiative.

Improve the national strategy for cybersecurity. In March 2009, we testified on needed improvements to the nation's cybersecurity strategy.[14]

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

In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 1.

Table 1: Key Strategy Improvement Identified by Cybersecurity Experts

1.	Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public-private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research and experience in this area. Until they are addressed, our nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

Since our March testimony, the Obama Administration has performed a review[15] of the strategy and issued a list of short and long term actions,

[15]The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

which are largely consistent with our past reports and recommendations, to strengthen the strategy. In response to one of these actions, the president appointed a cybersecurity coordinator in December 2009. We recently initiated a review to assess the progress made by the executive branch in implementing the report's recommendations.

In summary, while federal agencies continue to report increased compliance in implementing security training requirements, most federal agencies reported weaknesses in most types of information security controls. Additionally, agencies reported mixed progress in implementing key security measures while inspectors general identified persistent weaknesses in those areas of agencies' information security programs. There are multiple opportunities for the federal government to enhance federal cybersecurity and address these continuing weaknesses. These opportunities include addressing the hundreds of recommendations we and inspectors general have made to agencies, making enhancements to FISMA and its implementing guidance, and continuing efforts on White House, OMB, and federal agencies' initiatives. A concerted response by the federal government to current information security challenges will include acting on these opportunities; without such a response, federal information and systems will remain vulnerable.

Chairwoman Watson, this concludes my statement. I would be happy to answer any questions you or other members of the subcommittee may have.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Anjalique Lawrence (Assistant Director), Larry Crosland, Sharhonda Deloach, Kristi Dorsey, Rebecca Eyler, Nicole Jarvis, Linda Kochersberger, Mary Marshall, Minette Richardson, and Jayne Wilson.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548