United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, April 24, 2012

CYBERSECURITY

Threats Impacting the Nation

Statement of Gregory C. Wilshusen, Director
Information Security Issues

April 24, 2012

CYBERSECURITY

Threats Impacting the Nation

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-666T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Nearly every aspect of American society increasingly depends upon information technology systems and networks. This includes increasing computer interconnectivity, particularly through the widespread use of the Internet as a medium of communication and commerce. While providing significant benefits, this increased interconnectivity can also create vulnerabilities to cyber-based threats. Pervasive and sustained cyber attacks against the United States could have a potentially devastating impact on federal and nonfederal systems, disrupting the operations of governments and businesses and the lives of private individuals. Accordingly, GAO has designated federal information security as a governmentwide high-risk area since 1997, and in 2003 expanded it to include protecting systems and assets vital to the nation (referred to as critical infrastructures).

GAO is providing a statement that describes (1) cyber threats facing the nation's systems, (2) vulnerabilities present in federal information systems and systems supporting critical infrastructure, and (3) reported cyber incidents and their impacts. In preparing this statement, GAO relied on previously published work in these areas and reviewed more recent GAO, agency, and inspectors general work, as well as reports on security incidents.

What GAO Recommends

GAO has previously made recommendations to resolve identified significant control deficiencies.

View GAO-12-666T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The nation faces an evolving array of cyber-based threats arising from a variety of sources. These threats can be intentional or unintentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems, and intentional threats can be both targeted and untargeted attacks from a variety of threat sources. Sources of threats include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Moreover, potential threat actors have a variety of attack techniques at their disposal, which can adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. The nature of cyber attacks can vastly enhance their reach and impact due to the fact that attackers do not need to be physically close to their victims and can more easily remain anonymous, among other things. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals, businesses, critical infrastructures, or government organizations.

The threat posed by cyber attacks is heightened by vulnerabilities in federal systems and systems supporting critical infrastructure. Specifically, significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems supporting the operations, assets, and personnel of federal government agencies. For example, 18 of 24 major federal agencies have reported inadequate information security controls for financial reporting for fiscal year 2011, and inspectors general at 22 of these agencies identified information security as a major management challenge for their agency. Moreover, GAO, agency, and inspector general assessments of information security controls during fiscal year 2011 revealed that most major agencies had weaknesses in most major categories of information system controls. In addition, GAO has identified vulnerabilities in systems that monitor and control sensitive processes and physical functions supporting the nation's critical infrastructures. These and similar weaknesses can be exploited by threat actors, with potentially severe effects.

The number of cybersecurity incidents reported by federal agencies continues to rise, and recent incidents illustrate that these pose serious risk. Over the past 6 years, the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent. These incidents include unauthorized access to systems; improper use of computing resources; and the installation of malicious software, among others. Reported attacks and unintentional incidents involving federal, private, and infrastructure systems demonstrate that the impact of a serious attack could be significant, including loss of personal or sensitive information, disruption or destruction of critical infrastructure, and damage to national and economic security.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the cyber-based threats facing our nation.

The increasing dependency upon information technology (IT) systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependency can also create vulnerabilities to cyber-based threats. Pervasive and sustained cyber attacks against the United States could have a potentially devastating impact on federal and nonfederal systems and operations. In January 2012, the Director of National Intelligence testified that such threats pose a critical national and economic security concern.[1] These growing and evolving threats can potentially affect all segments of our society—individuals; private businesses; local, state, and federal governments; and other entities. Underscoring the importance of this issue, we have designated federal information security as a high-risk area since 1997 and in 2003 expanded this area to include protecting computerized systems supporting our nation's critical infrastructure.[2]

In my testimony today, I will describe (1) cyber threats facing the nation's systems, (2) vulnerabilities present in federal systems and systems supporting critical infrastructure,[3] and (3) reported cyber incidents and their impacts. In preparing this statement in April 2012, we relied on our previous work in these areas. (Please see the related GAO products in appendix I.) These products contain detailed overviews of the scope and methodology we used. We also reviewed more recent agency, inspector

[1]James R. Clapper, Director of National Intelligence, Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence (January 31, 2012).

[2]See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[3]Critical infrastructures are systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on national security, economic well-being, public health or safety, or any combination of these.

general, and GAO assessments of security vulnerabilities at federal agencies and information on security incidents from the U.S. Computer Emergency Readiness Team (US-CERT), media reports, and other publicly available sources. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits 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 provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, as well as developing into an extended information and communications infrastructure supporting vital services such as power distribution, health care, law enforcement, and national defense.

Consequently, the security of these systems and networks is essential to protecting national and economic security, public health and safety, and the flow of commerce. Conversely, ineffective information security controls can result in significant risks, including

- loss or theft of resources, such as federal payments and collections;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personal taxpayer information, or proprietary business information;
- disruption of critical operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government; and
- use of computer resources for unauthorized purposes or to launch attacks on other computers systems.

The Nation Faces an Evolving Array of Cyber-Based Threats

Cyber-based threats are evolving and growing and arise from a wide array of sources. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Table 1 shows common sources of cyber threats.

Table 1: Sources of Cybersecurity Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access 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, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, 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 could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.

Threat source	Description
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. 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, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

These sources of cyber threats make use of various techniques, or exploits, that may adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Table 2 provides descriptions of common types of cyber exploits.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.

Type of exploit	Description
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer– sometimes with a powerful antenna–searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

The unique nature of cyber-based attacks can vastly enhance their reach and impact. For example, cyber attackers do not need to be physically close to their victims, technology allows attacks to easily cross state and national borders, attacks can be carried out at high speed and directed at a number of victims simultaneously, and cyber attackers can more easily remain anonymous. Moreover, the use of these and other techniques is becoming more sophisticated, with attackers using multiple or "blended" approaches that combine two or more techniques. Using these techniques, threat actors may target individuals, resulting in loss of privacy or identity theft; businesses, resulting in the compromise of proprietary information or intellectual capital; critical infrastructures, resulting in their disruption or destruction; or government agencies, resulting in the loss of sensitive information and damage to economic and national security.

Systems Supporting Federal Operations and Critical Infrastructure Are Vulnerable to Cyber Attacks

Significant weaknesses in information security controls 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. For example, in their performance and accountability reports and annual financial reports for fiscal year 2011, 18 of 24 major federal agencies[4] indicated that inadequate information security controls were either material weaknesses or significant deficiencies[5] for financial reporting purposes. In addition, inspectors general at 22 of the major agencies identified information security or information system control as a major management challenge for their agency.

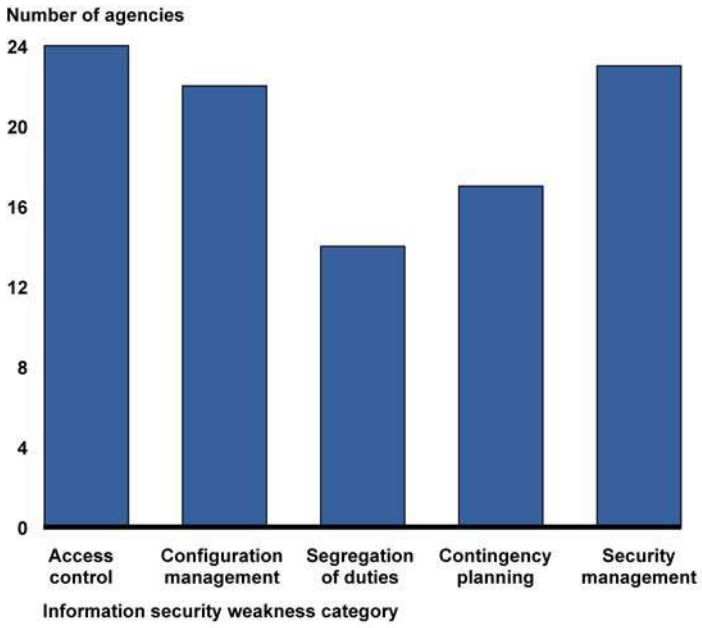
Agency, inspectors general, and GAO assessments of information security controls during fiscal year 2011 revealed that most major federal agencies had weaknesses in most of the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which helps avoid significant disruptions in computer-dependent operations; and (5) agencywide information security programs, which provide a framework for ensuring that risks are understood and that effective controls are selected and implemented. Figure 1 shows the

[4]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.

[5]A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. 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 and correct, misstatements on a timely basis.

number of agencies that had vulnerabilities in these five information security control categories.

Figure 1: Information Security Weaknesses at 24 Major Federal Agencies in Fiscal Year 2011



Source: GAO analysis of agency, inspectors general, and GAO reports.

Over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve similar previously identified significant control deficiencies. We have also recommended that agencies fully implement comprehensive, agencywide information security programs, including by correcting weaknesses in specific areas of their programs. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, securing the control systems that monitor and control sensitive processes and physical functions supporting many of our nation's critical infrastructures is a national priority, and we have identified vulnerabilities in these systems. For example, in September 2007, we reported that critical infrastructure control systems faced increasing risks due to cyber threats, system vulnerabilities, and the serious potential

impact of possible attacks.[6] Specifically, we determined that critical infrastructure owners faced both technical and organizational challenges to securing control systems, such as limited processing capabilities and developing compelling business cases for investing in control systems security, among others. We further identified federal initiatives under way to help secure these control systems, but noted that more needed to be done to coordinate these efforts and address shortfalls. We made recommendations to the Department of Homeland Security to develop a strategy for coordinating control systems security efforts and enhance information sharing with relevant stakeholders. Since this report, the department formed the Industrial Control Systems Cyber Emergency Response Team to provide industrial control system stakeholders with situational awareness and analytical support to effectively manage risk. In addition, it has taken several actions, such as developing a catalog of recommended security practices for control systems, developing a cybersecurity evaluation tool that allows asset owners to assess their control systems and overall security posture, and collaborating with others to promote control standards and system security. We have not evaluated these activities to assess their effectiveness in improving the security of control systems against cyber threats.

In May 2008, we reported that the Tennessee Valley Authority's (TVA) corporate network contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[7] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA's critical infrastructures and 73 recommendations to address weaknesses in information security controls. TVA concurred with the recommendations and has taken steps to implement them.

In addition to those present in federal systems and systems supporting critical infrastructure, vulnerabilities in mobile computing devices used by individuals or organizations may provide openings to cyber threats. For example, consumers and federal agencies are increasing their use of mobile devices to communicate and access services over the Internet.

[6]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).

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

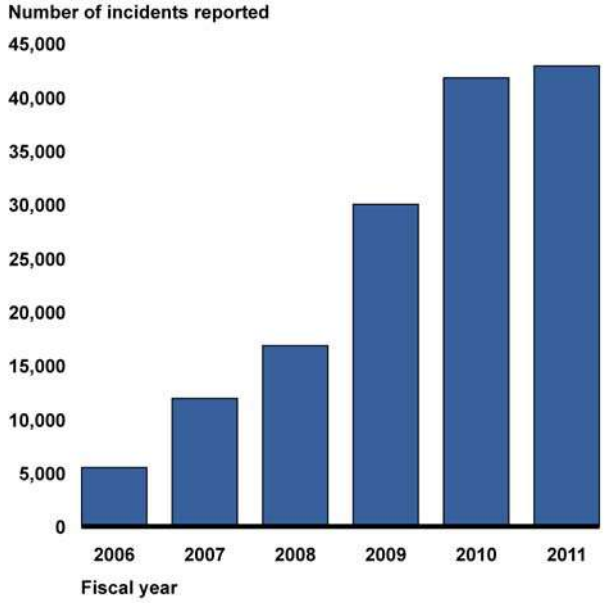
The use of these devices offers many benefits including ease of sending and checking messages and remotely accessing information online; however, it can also introduce information security risks if not properly protected. We have ongoing work to determine (1) what common security threats and vulnerabilities affect generally available cellphones, smartphones, and tablets; (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities; and (3) the extent to which government and private entities are addressing security vulnerabilities of mobile devices.

Number of Cybersecurity Incidents Reported by Federal Agencies Continues to Rise, and Recent Incidents Illustrate Serious Risk

Federal agencies have reported increasing numbers of security incidents that placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. When incidents occur, agencies are to notify the federal information security incident center—US-CERT. Over the past 6 years, the number of incidents reported by federal agencies to US-CERT has increased from 5,503 incidents in fiscal year 2006 to 42,887 incidents in fiscal year 2011, an increase of nearly 680 percent (see fig. 2).[8]

[8]According to US-CERT, the growth in the number of incidents is attributable, in part, to agencies improving detection and reporting of security incidents on their respective networks.

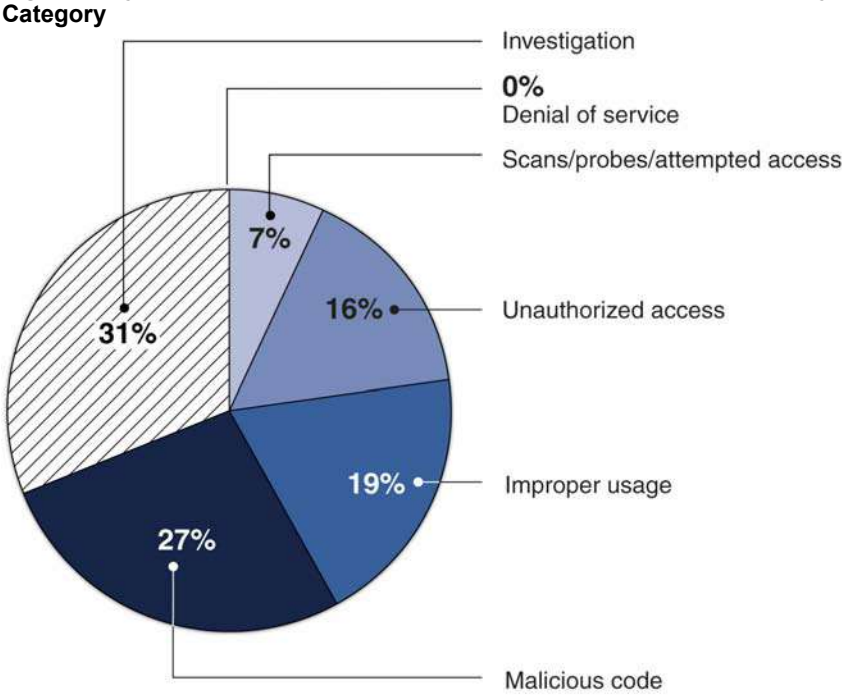
Figure 2: Incidents Reported to US-CERT: Fiscal Years 2006-2011



Source: GAO analysis of US-CERT data for fiscal years 2006-2011.

Agencies reported the types of incidents and events based on US-CERT-defined categories. As indicated in figure 3, the two most prevalent types of incidents and events reported to US-CERT during fiscal year 2011 were unconfirmed incidents under investigation and malicious code.

Figure 3: Types of Incidents Reported to US-CERT in Fiscal Year 2011 by Category



GAO analysis of US-CERT data for fiscal year 2011.

Reported attacks and unintentional incidents involving federal, private, and critical infrastructure systems demonstrate that the impact of a serious attack could be significant. These agencies and organizations have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples from news media and other public sources illustrate that a broad array of information and assets remain at risk.

- In April 2012, hackers breached a server at the Utah Department of Health to access thousands of Medicaid records. Included in the breach were Medicaid recipients and clients of the Children's Health Insurance Plan. About 280,000 people had their Social Security numbers exposed. In addition, another 350,000 people listed in the eligibility inquiries may have had other sensitive data stolen, including names, birth dates, and addresses.
- In March 2012, it was reported that a security breach at Global Payments, a firm that processed payments for Visa and Mastercard, could compromise the credit- and debit-card information of millions of Americans. Subsequent to the reported breach, the company's stock

fell more than 9 percent before trading in its stock was halted. Visa also removed the company from its list of approved processors.

- In February 2012, the inspector general at the National Aeronautics and Space Administration testified that an unencrypted notebook computer had been stolen from the agency in March 2011. The theft resulted in the loss of the algorithms used to command and control the International Space Station.
- In March 2012, a news wire service reported that the senior commander of the North Atlantic Treaty Organization (NATO) had been the target of repeated cyber attacks using the social networking website Facebook that were believed to have originated in China. According to the article, hackers repeatedly tried to dupe those close to the commander by setting up fake Facebook accounts in his name in the hope that his acquaintances would make contact and answer private messages, potentially divulging sensitive information about the commander or themselves.
- In March 2012, it was reported that Blue Cross Blue Shield of Tennessee paid out a settlement of $1.5 million to the U.S. Department of Health and Human Services arising from potential violations stemming from the theft of 57 unencrypted computer hard drives that contained protected health information of over 1 million individuals.
- In January 2012, the Department of Commerce discovered that the computer network of the department's Economic Development Administration (EDA) was hit with a virus, forcing EDA to disable e-mail services and Internet access pending investigation into the cause and scope of the problem, which persisted for over 12 weeks.
- In June 2011, a major bank reported that hackers had broken into its systems and gained access to the personal information of hundreds of thousands of customers. Through the bank's online banking system, the attackers were able to view certain private customer information.
- Citi reissued over 200,000 cards after a May 2011 website breach. About 360,000 of its approximately 23.5 million North American card accounts were affected, resulting in the potential for misuse of cardholder personal information.
- In April 2011, Sony disclosed that it suffered a massive breach in its video game online network that led to the theft of personal information, including the names, addresses, and possibly credit card data belonging to 77 million user accounts.
- In February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- In July 2010, a sophisticated computer attack, known as Stuxnet, was discovered. It targeted control systems used to operate industrial

processes in the energy, nuclear, and other critical sectors, reportedly causing physical damage. It is designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.

- A retailer reported in May 2011 that it had suffered a breach of its customers' card data. The company discovered tampering with the personal identification number (PIN) pads at its checkout lanes in stores across 20 states.
- In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, 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.

These incidents illustrate the serious impact that cyber threats can have on federal agency operations, the operations of critical infrastructures, and the security of sensitive personal and financial information.

In summary, the cyber-threats facing the nation are evolving and growing, with a wide array of potential threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities. The danger posed by these threats is heightened by the weaknesses that continue to exist in federal information systems and systems supporting critical infrastructures. Ensuring the security of these systems is critical to avoiding potentially devastating impacts, including loss, disclosure, or modification of personal or sensitive information; disruption or destruction of critical infrastructure; and damage to our national and economic security.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have at this time.

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 Michael Gilmore and Anjalique Lawrence (Assistant Directors), Kristi C. Dorsey, and Lee A. McCracken.

Appendix I: Related GAO Products

Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures. GAO-12-424R. Washington, D.C.: April 13, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO-12-361. Washington, D.C.: March 23, 2012.

Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data. GAO-12-393. Washington, D.C.: March 16, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid. GAO-12-507T. Washington, D.C.: February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. GAO-12-92. Washington, D.C.: December 9, 2011.

Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination. GAO-12-8. Washington, D.C.: November 29, 2011.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. GAO-12-130T. Washington, D.C.: October 6, 2011.

Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. GAO-12-137. Washington, D.C.: October 3, 2011.

Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards. GAO-11-751. Washington, D.C.: September 20, 2011.

Information Security: FDIC Has Made Progress, but Further Actions Are Needed to Protect Financial Data. GAO-11-708. Washington, D.C.: August 12, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. GAO-11-865T. Washington, D.C.: July 26, 2011.

Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities. GAO-11-75. Washington, D.C.: July 25, 2011.

Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain. GAO-11-149. Washington, D.C.: July 8, 2011.

Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate. GAO-11-605. Washington, D.C.: Jun 28, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems. GAO-11-463T. Washington, D.C.: March 16, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. GAO-11-117. Washington, D.C.: January 12, 2011.

Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk. GAO-11-43. Washington, D.C.: November 30, 2010.

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. GAO-11-24. Washington, D.C.: October 6, 2010.

Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems. GAO-10-916. Washington, D.C.: September 15, 2010.

Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies. GAO-10-872T. Washington, D.C.: July 22, 2010.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628. Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.

Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development. GAO-10-466. Washington, D.C.: June 3, 2010.

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. GAO-10-513. Washington, D.C.: May 27, 2010.

Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements. GAO-10-202. Washington, D.C.: March 12, 2010.

Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. GAO-10-237. Washington, D.C.: March 12, 2010.

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

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

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

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.