United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 11:00 a.m. EDT
July, 26, 2011

CYBERSECURITY

Continued Attention Needed to Protect Our Nation's Critical Infrastructure

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

July 26, 2011

CYBERSECURITY

Continued Attention Needed to Protect Our Nation's Critical Infrastructure

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-865T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

Increasing computer interconnectivity, such as the growth of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. However, this widespread interconnectivity poses significant risks to the government's and the nation's computer systems, and to the critical infrastructures they support. These critical infrastructures include systems and assets—both physical and virtual—that are essential to the nation's security, economic prosperity, and public health, such as financial institutions, telecommunications networks, and energy production and transmission facilities. Because most of these infrastructures are owned by the private sector, establishing effective public-private partnerships is essential to securing them from pervasive cyber-based threats. Federal law and policy call for federal entities, such as the Department of Homeland Security (DHS), to work with private-sector partners to enhance the physical and cyber security of these critical infrastructures.

GAO is providing a statement describing (1) cyber threats facing cyber-reliant critical infrastructures; (2) recent actions the federal government has taken, in partnership with the private sector, to identify and protect cyber-reliant critical infrastructures; and (3) ongoing challenges to protecting these infrastructures. In preparing this statement, GAO relied on its previously published work in the area.

View GAO-11-865T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In a February 2011 testimony, the Director of National Intelligence noted that there has been a dramatic increase in cyber activity targeting U.S. computers and systems in the last year, including a more than tripling of the volume of malicious software since 2009. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, or the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, hostile nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructure, the security of sensitive information, and the flow of commerce. Recent reported incidents include hackers accessing the personal information of hundreds of thousands of customers of a major U.S. bank and a sophisticated computer attack targeting control systems used to operate industrial processes in the energy, nuclear, and other critical sectors.

Over the past 2 years, the federal government, in partnership with the private sector, has taken a number of steps to address threats to cyber critical infrastructure. In early 2009, the White House conducted a review of the nation's cyberspace policy that addressed the missions and activities associated with the nation's information and communications infrastructure. The results of the review led, among other things, to the appointment of a national Cybersecurity Coordinator with responsibility for coordinating the nation's cybersecurity policies and activities. Also in 2009, DHS updated its National Infrastructure Protection Plan, which provides a framework for addressing threats to critical infrastructures and relies on a public-private partnership model for carrying out these efforts. DHS has also established a communications center to coordinate national response efforts to cyber attacks and work directly with other levels of government and the private sector and has conducted several cyber attack simulation exercises.

Despite recent actions taken, a number of significant challenges remain to enhancing the security of cyber-reliant critical infrastructures, such as

- implementing actions recommended by the president's cybersecurity policy review;
- updating the national strategy for securing the information and communications infrastructure;
- reassessing DHS's planning approach to critical infrastructure protection;
- strengthening public-private partnerships, particularly for information sharing;
- enhancing the national capability for cyber warning and analysis;
- addressing global aspects of cybersecurity and governance; and
- securing the modernized electricity grid, referred to as the "smart grid."

In prior reports, GAO has made many recommendations to address these challenges. GAO also continues to identify protecting the nation's cyber critical infrastructure as a governmentwide high-risk area.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the cybersecurity risks to the nation's critical infrastructure.

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. From its origins in the 1960s as a research project sponsored by the U.S. government, the Internet has grown increasingly important to both American and foreign businesses and consumers, serving as the medium for hundreds of billions of dollars of commerce each year. The Internet has also become an extended information and communications infrastructure, supporting vital services such as power distribution, health care, law enforcement, and national defense.

While the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, can allow unauthorized individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Recent cyber-based attacks have further underscored the need to manage and bolster the cybersecurity of our nation's critical infrastructures.

Mr. Chairman, in February, GAO issued its biennial high-risk list of government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges.[1] Once again, we identified protecting the federal government's information systems and the nation's cyber critical infrastructure as a governmentwide high-risk area. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure, referred to as cyber critical infrastructure protection or cyber CIP.

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

In my testimony today, I will describe (1) cyber threats facing cyber-reliant critical infrastructures; (2) recent actions the federal government has taken, in partnership with the private sector, to identify and protect cyber-reliant critical infrastructures; and (3) ongoing challenges to protecting cyber critical infrastructure. In preparing this statement in July 2011, we relied on our previous work in these areas (please see the related GAO products page at the end of this statement). These products contain detailed overviews of the scope of our reviews and the methodology we used. The work on which this statement 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 evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

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, pubic health or safety, or any combination of these. Critical infrastructure includes, among other things, banking and financial institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned by the private sector. As these critical infrastructures have become increasingly dependent on computer systems and networks, the interconnectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt critical systems, with potentially harmful effects.

Because the private sector owns most of the nation's critical infrastructures, forming effective partnerships between the public and private sectors is vital to successfully protect cyber-reliant critical assets from a multitude of threats, including terrorists, criminals, and hostile nations. Federal law and policy have established roles and responsibilities for federal agencies to work with the private sector and other entities in enhancing the cyber and physical security of critical public and private infrastructures. These policies stress the importance of coordination between the government and the private sector to protect the nation's computer-reliant critical infrastructure. In addition, they establish the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation efforts, and recovery efforts for public and private critical infrastructure and information systems. Federal

policy also establishes critical infrastructure sectors, assigns federal agencies to each sector (known as sector lead agencies), and encourages private sector involvement. Table 1 shows the 18 critical infrastructure sectors and the lead agencies assigned to each sector.

Table 1: Critical Infrastructure Sectors and Lead Agencies

Critical infrastructure sector	Description	Lead agency or agencies
Agriculture and food	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	Department of Agriculture Department of Health and Human Services (Food and Drug Administration)
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.	Department of the Treasury
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	DHS
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	DHS
Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS
Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.	DHS
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	DHS
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	DHS
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the U.S. and abroad.	DHS

Critical infrastructure sector	Description	Lead agency or agencies
Health care and public health	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS
National monuments and icons	Maintains monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.	Department of the Interior
Nuclear reactors, materials, and waste	Provides nuclear power. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.	DHS
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector	DHS
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	DHS
Water	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.	Environmental Protection Agency

Source: GAO-08-1075R, GAO-11-537R.

In May 1998, Presidential Decision Directive 63 (PDD-63) established critical infrastructure protection as a national goal and presented a strategy for cooperative efforts by the government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government.[2] Among other things, this directive encouraged the development of information sharing and analysis centers (ISAC) to serve as mechanisms for gathering, analyzing, and disseminating information on cyber infrastructure threats and vulnerabilities to and from owners and operators of the sectors and the federal government. For example, the Financial Services, Electricity Sector, IT, and Communications ISACs represent sectors or subcomponents of sectors.

[2]The White House, *Presidential Decision Directive/NSC 63* (Washington, D.C.: May 22, 1998).

The Homeland Security Act of 2002 created the Department of Homeland Security.[3] Among other things, DHS was assigned with the following critical infrastructure protection responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States, (2) recommending measures to protect those key resources and critical infrastructures in coordination with other groups, and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks.

In 2003, the *National Strategy to Secure Cyberspace* was issued, which assigned DHS multiple leadership roles and responsibilities in protecting the nation's cyber critical infrastructure.[4] These include (1) developing a comprehensive national plan for critical infrastructure protection; (2) developing and enhancing national cyber analysis and warning capabilities; (3) providing and coordinating incident response and recovery planning, including conducting incident response exercises; (4) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems; and (5) strengthening international cyberspace security.

PDD-63 was superseded in December 2003 when Homeland Security Presidential Directive 7 (HSPD-7) was issued.[5] HSPD-7 defined additional responsibilities for DHS, sector-specific agencies, and other departments and agencies. The directive instructs sector-specific agencies to identify, prioritize, and coordinate the protection of critical infrastructures to prevent, deter, and mitigate the effects of attacks. It also makes DHS responsible for, among other things, coordinating national critical infrastructure protection efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.

[3]Homeland Security Act of 2002, Pub. L. No. 107-296 (Nov. 25, 2002).

[4]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

[5]The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: December 17, 2003).

As part of its implementation of the cyberspace strategy and other requirements to establish cyber analysis and warning capabilities for the nation, DHS established the United States Computer Emergency Readiness Team (US-CERT) to help protect the nation's information infrastructure. US-CERT is the focal point for the government's interaction with federal and private-sector entities 24 hours a day, 7 days a week, and provides cyber-related analysis, warning, information-sharing, major incident response, and national-level recovery efforts.

Cyber-Reliant Critical Infrastructures Face a Proliferation of Threats

Threats to systems supporting critical infrastructure are evolving and growing. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[6] Different types of cyber threats from numerous sources may adversely affect computers, software, networks, organizations, entire industries, or the Internet itself. Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures 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.

The potential impact of these threats is amplified by the connectivity between information systems, the Internet, and other infrastructures, creating opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. For example, 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

[6]Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community, statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

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

infrastructures and 73 recommendations to address specific weaknesses in security controls. TVA concurred with the recommendations and has taken steps to implement them. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Recent reports of cyber attacks illustrate that the cyber-based attacks on cyber-reliant critical infrastructures could have a debilitating impact on national and economic security.

- In June 2011, a major bank reported that hackers broke 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.

- In March 2011, according to the Deputy Secretary of Defense, a cyber attack on a defense company's network captured 24,000 files containing Defense Department information. He added that nations typically launch such attacks, but there is a growing risk of terrorist groups and rogue states developing similar capabilities.

- In March 2011, a security company reported that it had suffered a sophisticated cyber attack that removed information about its two-factor authentication tool.[8] According to the company, the extracted information did not enable successful direct attacks on any of its customers; however, the information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack.

- In February 2011, media reports stated that computer hackers broke into and stole 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. It is

[8]Two-factor authentication is a way of verifying someone's identity by using two of the following: something the user knows (password), something the user has (token), or something unique to the user (fingerprint).

designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.

- In January 2010, it was reported that at least 30 technology companies—most in Silicon Valley, California—were victims of intrusions. The cyber attackers infected computers with hidden programs allowing unauthorized access to files that may have included the companies' computer security systems, crucial corporate data, and software source code.

The Federal Government Has Taken Steps to Address Cyber Threats to Cyber Critical Infrastructure

Over the past 2 years, the federal government has taken a number of steps aimed at addressing cyber threats to critical infrastructure.

In early 2009, the President initiated a review of the nation's cyberspace policy that specifically assessed the missions and activities associated with the nation's information and communication infrastructure and issued the results in May of that year.[9] The review resulted in 24 near- and mid-term recommendations to address organizational and policy changes to improve the current U.S. approach to cybersecurity. These included, among other things, that the President appoint a cybersecurity policy official for coordinating the nation's cybersecurity policies and activities. In December 2009, the President appointed a Special Assistant to the President and Cybersecurity Coordinator to serve in this role and act as the central coordinator for the nation's cybersecurity policies and activities. Among other things, this official is to chair the primary policy coordination body within the Executive Office of the President responsible for directing and overseeing issues related to achieving a reliable global information and communications infrastructure.

Also in 2009, DHS issued an updated version of its National Infrastructure Protection Plan (NIPP). The NIPP is intended to provide the framework for a coordinated national approach to addressing the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation's critical infrastructures. The NIPP relies on a sector partnership model as the primary means of coordinating government and private-sector critical infrastructure protection efforts. Under this model, each sector has both a government council and a private sector council to

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

address sector-specific planning and coordination. The government and private-sector councils are to work in tandem to create the context, framework, and support for the coordination and information-sharing activities required to implement and sustain each sector's infrastructure protection efforts. The council framework allows for the involvement of representatives from all levels of government and the private sector, to facilitate collaboration and information-sharing in order to assess events accurately, formulate risk assessments, and determine appropriate protective measures. The establishment of private-sector councils is encouraged under the NIPP model, and these councils are to be the principal entities for coordinating with the government on a wide range of CIP activities and issues. Using the NIPP partnership model, the private and public sectors coordinate to manage the risks related to cyber CIP by, among other things, sharing information, providing resources, and conducting exercises.

In October 2009, DHS established its National Cybersecurity and Communications Integration Center (NCCIC) to coordinate national response efforts and work directly with federal, state, local, tribal, and territorial governments and private-sector partners. The NCCIC integrates the functions of the National Cyber Security Center, US-CERT, the National Coordinating Center for Telecommunications, and the Industrial Control Systems CERT into a single coordination and integration center and co-locates other essential public and private sector cybersecurity partners.

In September 2010, DHS issued an interim version of its national cyber incident response plan. The purpose of the plan is to establish the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident. It aims to tie various policies and doctrine together into a single tailored, strategic, cyber-specific plan designed to assist with operational execution, planning, and preparedness activities and to guide short-term recovery efforts.

DHS has also coordinated several cyber attack simulation exercises to strengthen public and private incident response capabilities. In September 2010, DHS conducted the third of its Cyber Storm exercises, which are large-scale simulations of multiple concurrent cyber attacks. (DHS previously conducted Cyber Storm exercises in 2006 and 2008.) The third Cyber Storm exercise was undertaken to test the National Cyber Incident Response Plan, and its participants included

representatives from federal departments and agencies, states, ISACs, foreign countries, and the private sector.

Challenges in Protecting Cyber Critical Infrastructure Persist

Despite the actions taken by several successive administrations and the executive branch agencies, significant challenges remain to enhancing the protection of cyber-reliant critical infrastructures.

- *Implementing actions recommended by the president's cybersecurity policy review.* In October 2010, we reported that of the 24 near- and mid-term recommendations made by the presidentially initiated policy review to improve the current U.S. approach to cybersecurity, only 2 had been implemented and 22 were partially implemented.[10] Officials from key agencies involved in these efforts (e.g., DHS, the Department of Defense, and the Office of Management and Budget) stated that progress had been slower than expected because agencies lacked assigned roles and responsibilities and because several of the mid-term recommendations would require action over multiple years. We recommended that the national Cybersecurity Coordinator designate roles and responsibilities for each recommendation and develop milestones and plans, including measures, to show agencies' progress and performance.

- *Updating the national strategy for securing the information and communications infrastructure*. In March 2009, we testified on the needed improvements to the nation's cybersecurity strategy.[11] In preparation for that testimony, we convened a panel of experts that included former federal officials, academics, and private-sector executives. The panel highlighted 12 key improvements that, in its view, were essential to improving the strategy and our national cybersecurity postures, including (1) the development of a national strategy that clearly articulates objectives, goals, and priorities; (2) focusing more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing plans;

[10]GAO, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (Washington, D.C.: Oct. 6, 2010).

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

and (3) bolstering public-private partnerships though an improved value proposition and use of incentives.

- *Reassessing the cyber sector-specific planning approach to critical infrastructure protection*. In September 2009, we reported that, among other things, sector-specific agencies had yet to update their respective sector-specific plans to fully address key DHS cyber security criteria.[12] In addition, most agencies had not updated the actions and reported progress in implementing them as called for by DHS guidance. We noted that these shortfalls were evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where it stands in securing cyber critical infrastructures. We recommended that DHS (1) assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure and consider whether other options would provide more effective results and (2) collaborate with the sectors to develop plans that fully address cyber security requirements. DHS concurred with the recommendations and has taken action to address them. For example, the department reported that it undertook a study in 2009 that determined that the existing sector-specific planning process, in conjunction with other related efforts planned and underway, should continue to be the nation's approach. In addition, at about this time, the department met and worked with sector officials to update sector plans with the goal of fully addressing cyber-related requirements.

- *Strengthening the public-private partnerships for securing cyber-critical infrastructure*. The expectations of private sector stakeholders are not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. In July 2010, we reported that federal partners, such as DHS, were taking steps that may address the key expectations of the private sector, including developing new information-sharing arrangements.[13] We also reported that public sector stakeholders believed that improvements could be made to the partnership, including improving

[12]GAO, *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*, GAO-09-969 (Washington, D.C.: September 24, 2009).

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

private sector sharing of sensitive information. We recommended, among other things, that the national Cybersecurity Coordinator and DHS work with their federal and private-sector partners to enhance information-sharing efforts, including leveraging a central focal point for sharing information among the private sector, civilian government, law enforcement, the military, and the intelligence community. DHS concurred with this recommendation and officials stated that they have made progress in addressing the recommendation. We will be determining the extent of that progress as part of our audit follow-up efforts.

- *Enhancing cyber analysis and warning capabilities*. DHS's US-CERT has not fully addressed 15 key attributes of cyber analysis and warning capabilities that we identified.[14] As a result, we recommended in July 2008 that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations and has reported that it is taking steps to implement them. We are currently working with DHS officials to determine the status of their efforts to address these recommendations.

- *Addressing global cybersecurity and governance*. Based on our review, the U.S. government faces a number of challenges in formulating and implementing a coherent approach to global aspects of cyberspace, including, among other things, providing top-level leadership, developing a comprehensive strategy, and ensuring cyberspace-related technical standards and policies do not pose unnecessary barriers to U.S. trade.[15] Specifically, we determined that the national Cybersecurity Coordinator's authority and capacity to effectively coordinate and forge a coherent national approach to cybersecurity were still under development. In addition, the U.S. government had not documented a clear vision of how the international efforts of federal entities, taken together, support overarching national goals. Further, we learned that some countries had attempted to mandate compliance with their indigenously

[14]GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

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

developed cybersecurity standards in a manner that risked discriminating against U.S. companies. We recommended that, among other things, the Cybersecurity Coordinator develop with other relevant entities a comprehensive U.S. global cyberspace strategy that, among other things, addresses technical standards and policies while taking into consideration U.S. trade. In May 2011, the White House released the *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. We will be determining the extent that this strategy addresses our recommendation as part of our audit follow-up efforts.

- *Securing the modernized electricity grid.* In January 2011, we reported on progress and challenges in developing, adopting, and monitoring cybersecurity guidelines for the modernized, IT-reliant electricity grid (referred to as the "smart grid").[16] Among other things, we identified six key challenges to securing smart grid systems. These included, among others,

  - a lack of security features being built into certain smart grid systems,
  - a lack of an effective mechanism for sharing information on cybersecurity within the electric industry, and
  - a lack of electricity industry metrics for evaluating cybersecurity.

  We also reported that the Department of Commerce's National Institute for Standards and Technology (NIST) had developed and issued a first version of its smart grid cybersecurity guidelines. While NIST largely addressed key cybersecurity elements that it had planned to include in the guidelines, it did not address an important element essential to securing smart grid systems that it had planned to include—addressing the risk of attacks that use both cyber and physical means. NIST officials said that they intend to update the guidelines to address the missing elements, and have drafted a plan to do so. While a positive step, the plan and schedule were still in draft form. We recommended that NIST finalize its plan and schedule

[16]GAO, *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).

for updating its cybersecurity guidelines to incorporate missing elements; NIST agreed with this recommendation.

In addition to the challenges we have previously identified, we have ongoing work in two key areas related to the protection of cyber critical infrastructures. The first is to identify the extent to which cybersecurity guidance has been specified within selected critical infrastructure sectors and to identify areas of commonality and difference between sector-specific guidance and guidance applicable to federal agencies. The second is a study of risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services, along with the extent to which national security-related agencies are taking risk-based approaches to supply-chain management. We plan to issue the results of this work in November 2011 and early 2012, respectively.

In summary, the threats to information systems are evolving and growing, and systems supporting our nation's critical infrastructure are not sufficiently protected to consistently thwart the threats. While actions have been taken, the administration and executive branch agencies need to address the challenges in this area to improve our nation's cybersecurity posture, including enhancing cyber analysis and warning capabilities and strengthening the public-private partnerships for securing cyber-critical infrastructure. Until these actions are taken, our nation's cyber critical infrastructure will remain vulnerable. Mr. Chairman, this completes my statement. I would be happy to answer any questions you or other members of the Subcommittee 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 (Assistant Director), Bradley Becker, Kami Corbett, and Lee McCracken.

Related GAO Products

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.

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

Critical Infrastructure Protection: *DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise.* GAO-08-825. Washington, D.C.: September 9, 2008.

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

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