United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2010

CRITICAL INFRASTRUCTURE PROTECTION

Key Private and Public Cyber Expectations Need to Be Consistently Addressed

GAO-10-628

July 2010

CRITICAL INFRASTRUCTURE PROTECTION

Key Private and Public Cyber Expectations Need to Be Consistently Addressed

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-628, a report to congressional requesters

Why GAO Did This Study

Pervasive and sustained computer-based attacks pose a potentially devastating impact to systems and operations and the critical infrastructures they support. Addressing these threats depends on effective partnerships between the government and private sector owners and operators of critical infrastructure. Federal policy, including the Department of Homeland Security's (DHS) National Infrastructure Protection Plan, calls for a partnership model that includes public and private councils to coordinate policy and information sharing and analysis centers to gather and disseminate information on threats to physical and cyber-related infrastructure. GAO was asked to determine (1) private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met. To do this, GAO conducted surveys and interviews of public and private sector officials and analyzed relevant policies and other documents.

What GAO Recommends

GAO recommends that the national Cybersecurity Coordinator and DHS work with their federal and private sector partners to enhance information-sharing efforts. The national Cybersecurity Coordinator provided no comments on a draft of this report. DHS concurred with GAO's recommendations.

View GAO-10-628 or key components.
For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Private sector stakeholders reported that they expect their federal partners to provide usable, timely, and actionable cyber threat information and alerts; access to sensitive or classified information; a secure mechanism for sharing information; security clearances; and a single centralized government cybersecurity organization to coordinate government efforts. However, according to private sector stakeholders, federal partners are not consistently meeting these expectations. For example, less than one-third of private sector respondents reported that they were receiving actionable cyber threat information and alerts to a great or moderate extent. (See table below.) Federal partners are taking steps that may address the key expectations of the private sector, including developing new information-sharing arrangements. However, while the ongoing efforts may address the public sector's ability to meet the private sector's expectations, much work remains to fully implement improved information sharing.

Private Sector Expected Services and the Extent to Which They Are Met

Services	Greatly or moderately expected	Greatly or moderately received
Timely and actionable cyber threat information	98%	27%
Timely and actionable cyber alerts	96%	27%
Access to actionable classified or sensitive information (such as intelligence and law enforcement information)	87%	16%
A secure information-sharing mechanism	78%	21%

Source: GAO analysis based on survey data of 56 private sector respondents.

Public sector stakeholders reported that they expect the private sector to provide a commitment to execute plans and recommendations, timely and actionable cyber threat information and alerts, and appropriate staff and resources. Four of the five public sector councils that GAO held structured interviews with reported that their respective private sector partners are committed to executing plans and recommendations and providing timely and actionable information. However, public sector council officials stated that improvements could be made to the partnership, including improving private sector sharing of sensitive information. Some private sector stakeholders do not want to share their proprietary information with the federal government for fear of public disclosure and potential loss of market share, among other reasons.

Without improvements in meeting private and public sector expectations, the partnerships will remain less than optimal, and there is a risk that owners of critical infrastructure will not have the information necessary to thwart cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure.

Contents

Abbreviations

CIP	critical infrastructure protection
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOE	Department of Energy
DOD	Department of Defense
HSPD-7	Homeland Security Presidential Directive 7
IT	information technology
ISAC	information-sharing and analysis center
NIPP	National Infrastructure Protection Plan
PDD-63	Presidential Decision Directive 63
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 15, 2010

Congressional Requesters

Recent cyber attacks on corporations of the United States and federal agencies highlight the threats posed by the worldwide connection of our networks. Because the private sector owns most of the nation's critical infrastructure—such as banking and financial institutions, telecommunications networks, and energy production and transmission facilities—it is vital that the public and private sectors form effective partnerships to successfully protect these cyber-reliant critical assets from a multitude of threats including terrorists, criminals, and hostile nations.[1]

Federal policy establishes various mechanisms for the development of public-private partnerships. The National Infrastructure Protection Plan (NIPP) describes a partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure.[2] For each sector, the model requires formation of government coordinating councils (government councils)—composed of federal, state, local, or tribal agencies with purview over critical sectors—and encourages voluntary formation of sector coordinating councils (sector councils)—composed of owner-operators of these critical assets (some of which may be state or local agencies) or their respective trade associations.[3] These councils create the structure through which representative groups from all levels of government and the private sector are to collaborate in planning and implementing efforts to protect critical infrastructure. The sector councils are envisioned to be policy-related and to represent a primary point of contact for government to plan the entire

[1]Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

[2]Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* (2009).

[3]Federal policy established 18 critical infrastructure sectors: agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, public health and health care, transportation systems, and water.

range of infrastructure protection activities, including those associated with mitigating cyber threats. The councils' functions are distinct from those of the private sector information-sharing and analysis centers (ISAC) that were established to serve an operational role such as providing mechanisms for gathering, analyzing, and disseminating information on physical and cyber-related infrastructure threats and vulnerabilities to and from private infrastructure sectors and the government.

Our objectives were to determine (1) private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met.[4]

To determine private sector expectations and to what extent these expectations are being met, we collected and analyzed documents related to the formation of public-private partnerships and their actions, conducted structured interviews, and surveyed 56 private sector representatives from the following cyber-reliant critical infrastructure sectors: (1) banking and finance, (2) communications, (3) defense industrial base (DIB), (4) energy, and (5) information technology (IT). The surveyed representatives were members of the ISACs and sector councils and were solicited by the leadership of those organizations to participate in our survey. To determine public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met, we collected and analyzed various documents and conducted structured interviews with government councils' representatives associated with the same cyber-reliant critical sectors mentioned above. We also interviewed several additional individuals with specialized expertise in the cyber-critical infrastructure protection public-private partnership model. Our findings and conclusions are based on information gathered from the five cyber-reliant critical sectors and are not generalizable to a larger population. Further details of our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from June 2009 to July 2010, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient,

[4]For the purposes of this report, private sector may include some nonprivate-sector entities, such as state, local, territorial, and tribal governments.

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

Public and private organizations rely on computer systems to transfer increasing amounts of money; sensitive, proprietary economic and commercial information; and classified and sensitive but unclassified defense and intelligence information. The increased transfer of critical information increases the risk that malicious individuals will attempt to disrupt or disable our nation's critical infrastructures and obtain sensitive and critical information for malicious purposes. To address the threats to the nation's cyber-reliant critical infrastructure, federal policy emphasizes the importance of public-private coordination.

Cyber Threats and Incidents Adversely Affect the Nation's Critical Infrastructure

Different types of cyber threats from numerous sources may adversely affect computers, software, a network, an agency's operations, an industry, 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. Attacks can come from a variety of sources, including criminal groups, hackers, and terrorists. Table 1 lists sources of threats that have been identified by the U.S. intelligence community and others.

Table 1: Sources of Cybersecurity Threats

Threat	Description
Bot-network operators	Bot-network 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 servers 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 and online fraud. International corporate spies and organized 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 others, and monetary gain, 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 also includes contractors hired by the organization, as well as employees who accidentally 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 U.S. citizens across the country.
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/malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/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 U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

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

Different types of cyber threats can use various cyber exploits that may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself (see table 2). Groups or individuals may

intentionally deploy cyber exploits targeting a specific cyber asset or attack through the Internet using a virus, worm, or malware with no specific target.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Denial-of-service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed denial-of-service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vishing	A method of phishing based on voice-over-Internet-Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem, and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

Sources: GAO analysis of data from GAO and industry reports.

Recent reports of cyber attacks illustrate that such attacks could have a debilitating impact on national and economic security and on public health and safety.

- In May 2007, Estonia was the reported target of a denial-of-service cyber attack with national consequences. The coordinated attack created mass outages of its government and commercial Web sites.[5]

- In March 2008, the Department of Defense (DOD) reported that, in 2007, computer networks operated by the department, other federal agencies, and defense-related think tanks and contractors were targets of computer network intrusion. Although those responsible were not definitively identified, the attacks appeared to have originated in China.[6]

- In January 2010, it was reported that at least 30 technology companies—most in Silicon Valley, California—were victims of intrusions. The cyber attackers gained unauthorized access to files that may have included the companies' computer security systems, crucial corporate data, and software source code.[7]

- In January 2010, a California-based company filed suit alleging that two Chinese companies stole software code and then distributed it to tens of millions of end users as part of Chinese government-sponsored filtering software. The company is seeking more than $2.2 billion dollars. Academic researchers found that portions of the company's software code had been copied and used in initial versions of the Chinese software.[8]

- Based on an 8-month investigation, researchers reported that computer systems in India were attacked. The suspected cyberattackers remotely connected to Indian computers using social networks to install bot-networks that infiltrated and infected Indian computers with malware. The incidents were reported to have been traced back to an underground espionage organization that was able to steal sensitive national security and defense information.[9]

[5]Computer Emergency Response Team of Estonia, "Malicious Cyber Attacks Against Estonia Come from Abroad" (Apr. 29, 2007) and Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference (Apr. 8, 2008).

[6]Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008*.

[7]The New York Times, *Google, Citing Attack, Threatens to Exit China* (Jan. 13, 2010).

[8]The New York Times, *Suit Says 2 Chinese Firms Stole Web-Blocking Code* (Jan. 7, 2010).

[9]The New York Times, *China Cyber–Spies Target India, Dalai Lama: Report* (Apr. 6, 2010).

Critical Infrastructure Protection Policy Emphasizes Private and Public Sector Coordination

Federal law and policy call for critical infrastructure protection activities that are intended to enhance the cyber and physical security of both the public and private infrastructures that are essential to national security, national economic security, and national public health and safety. Federal policies address the importance of coordination between the government and the private sector to protect the nation's computer-reliant critical infrastructure. These policies establish critical infrastructure sectors, assign agencies to each sector (sector lead agencies), and encourage private sector involvement. For example, the Department of the Treasury is responsible for the banking and finance sector, while the Department of Energy (DOE) is responsible for the energy sector. Table 3 lists agencies and their assigned sector.

Table 3: Sector-Specific Agencies and Assigned Sectors

Sector-specific agency	Critical infrastructure sector
Department of Agriculture Department of Health and Human Services	Agriculture and food
Department of Defense	DIB
Department of Energy	Energy
Department of Health and Human Services	Health care and public health
Department of the Interior	National monuments and icons
Department of the Treasury	Banking and finance
Department of Homeland Security	Chemical Commercial facilities Critical manufacturing Dams Emergency services Nuclear reactors, materials, and waste IT Communications Postal and shipping Transportation systems Government facilities
Environmental Protection Agency	Water

Source: National Infrastructure Protection Plan.

In May 1998, Presidential Decision Directive 63 (PDD-63) established critical infrastructure protection (CIP) 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.[10] Among other things, this directive encouraged the development of ISACs 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. However, not all sectors have ISACs. For example, according to private sector officials, the DIB sector and the subcomponents of the energy sector, besides electricity, do not have established ISACs.

The Homeland Security Act of 2002 created the Department of Homeland Security (DHS).[11] In addition, among other things, it assigned the department the following CIP responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States; (2) recommending measures to protect the key resources and critical infrastructures of the United States 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 this CIP area.[12] They include (1) developing a comprehensive national plan for CIP, including cybersecurity; (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.[13] HSPD-7 defined additional

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

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

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

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

responsibilities for DHS, federal agencies focused on specific critical infrastructure sectors (sector-specific agencies), and other departments and agencies. HSPD-7 instructs these sector-specific agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. HSPD-7 makes DHS responsible for, among other things, coordinating national CIP efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.

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. It is charged with aggregating and disseminating cybersecurity information to improve warning of and response to incidents, increasing coordination of response information, reducing vulnerabilities, and enhancing prevention and protection. In addition, the organization is to collect incident reports from all federal agencies and assist agencies in their incident response efforts. It is also to accept incident reports when voluntarily submitted by other public and private entities and assist them in their response efforts, as requested.

In addition, as part of its responsibilities, DHS first issued the NIPP in 2006 and then updated it in 2009. The NIPP is intended to provide the framework for a coordinated national approach to address the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation's critical infrastructure. The NIPP relies on a sector partnership model as the primary means of coordinating government and private sector CIP efforts. Under this model, each sector has both a government council and a private sector council to 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 coordination and information-sharing activities required to implement and sustain that sector's CIP efforts. The council framework allows for the involvement of representatives from all levels of government and the private sector, so that collaboration and information-sharing can occur to assess events accurately, formulate risk assessments, and determine appropriate protective measures.

The government councils are to coordinate strategies, activities, policies, and communications across government entities within each sector. Each government council is to be composed of representatives from various levels of government (i.e., federal, state, local, and tribal) as appropriate to the security needs of each individual sector. In addition, a representative from the sector-specific agency is to chair the council and is to provide cross-sector coordination with each of the member governments. For example, DOE in its role as the sector-specific agency for the energy sector has established and chairs a government council.

The establishment of private sector councils (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. Under the model, critical asset owners and operators are encouraged to be involved in the creation of sector councils that are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership can vary from sector to sector but should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within the sector. For example, the banking and finance sector has established the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, which is made up of over 40 entities, including banks, insurance companies, and industry associations.

Most recently, the White House issued the Cyberspace Policy Review that, among other things, recommended that the White House appoint a cybersecurity policy official for coordinating the nation's cybersecurity policies and activities.[14] Subsequently, in December 2009, the President appointed a Special Assistant to the President and Cybersecurity Coordinator, referred to as the Cybersecurity Coordinator in this report, to be the central coordinator of federal government cybersecurity-related activities.

Using the NIPP partnership model, the private and public sectors coordinate to manage the risks related to cyber CIP. This coordination includes sharing information, conducting exercises, and providing resources.

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

- *Sharing information.* Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. This includes sharing information on cyber threats and vulnerabilities, providing alerts or warnings about such threats, and recommending mitigation steps.

- *Conducting exercises.* Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between stakeholders in the context of serious cyber attacks, terrorist incidents, natural disasters, and other emergencies. Exercises are conducted by private sector owners and operators, and across all levels of government.

- *Providing resources.* Maximizing the efficient use of resources is a key part of protecting the nation's critical infrastructure. This includes providing technical and policy expertise, training, commitment of people, and financial aid through grants.

Previous GAO Work Made Recommendations to DHS and Identified Best Practices to Improve Public-Private Partnerships

Over the last several years, we have reported and made recommendations regarding various aspects of cyber CIP, including identifying information-sharing practices and bolstering the public-private partnership. In 2001, we identified the information-sharing practices of leading organizations and the factors they deemed critical to their success in building successful information-sharing relationships.[15] All of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships. Other critical success factors identified included (1) establishing effective and appropriately secure communication mechanisms, such as regular meetings and secure Web sites; (2) obtaining the support of senior managers at member organizations regarding the sharing of potentially sensitive member information and the commitment of resources; and (3) ensuring organizational leadership continuity. In addition, to be successful, information-sharing organizations provided identifiable membership benefits, such as current information about threats, vulnerabilities, and incidents. Without such benefits, according to the representatives we met with, members would not continue participating.

[15]GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington D.C: Oct. 15, 2001).

Over the last several years, we have also made about 30 recommendations in key cybersecurity areas to help bolster private-public partnerships. In 2008, we reported[16] on US-CERT and found that it faced a number of challenges that impeded it from fully implementing a cyber analysis and warning capability and thus being able to coordinate the national efforts to prepare for, prevent, and respond to cyber threats. The challenges included creating warnings that are consistently actionable and timely and employing predictive analysis. We made 10 recommendations to DHS to improve the department's cyber analysis and warning capabilities. These included, among others, addressing deficiencies in its monitoring efforts, including establishing a comprehensive baseline understanding of the nation's critical information infrastructure and engaging appropriate private-sector stakeholders to support a national-level cyber monitoring capability. We also recommended that DHS address the challenges that impeded it in fully implementing cyber analysis and warning, including developing close working relationships with federal and private-sector entities to allow the free flow of information and ensuring consistent notifications that are actionable and timely. DHS agreed with most of these recommendations and initiated related actions.

In 2007 and 2009, we determined the extent to which sector plans for CIP fully addressed DHS's cyber security requirements and assessed whether these plans and related reports provided for effective implementation.[17] We found, among other things, that although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies had yet to update their respective sector-specific plans to fully address key DHS cybersecurity criteria. The lack of complete updates and progress reports was further evidence that the sector planning process had not been effective, thus leaving the nation in the position of not knowing precisely where it stands in securing cyber-critical infrastructures. Not following up to address these conditions also showed DHS was not making sector planning a priority. We recommended that DHS assess whether the existing sector-specific planning process should continue to be the nation's approach to securing cyber and other

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

[17]GAO, *Critical Infrastructure Protection: Sector-specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington D.C.: Oct. 31, 2007) and *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*, GAO-09-969 (Washington D.C.: Sept. 24, 2009).

critical infrastructure and, if so, make the process an agency priority and manage it accordingly. DHS concurred with the recommendations. In addition, due to concerns about DHS's efforts to fully implement its CIP responsibilities, as well as known security risks to critical infrastructure systems, we added cyber CIP as part of our federal IT systems security high-risk area in 2003 and have continued to report on its status since that time.[18]

Most recently, we testified in 2009 on the results of expert panels that identified the importance of bolstering public-private partnerships.[19] In discussions with us, the panel identified 12 key areas requiring improvement. One of the key strategies was to bolster public-private partnerships by providing adequate economic and other incentives for greater investment and partnering in cybersecurity.

Private Sector Stakeholders Expect Information on Threats, Alerts, and Other Related Services but Believe Federal Partners Are Not Consistently Providing

Private sector stakeholders—sector council and ISAC members—reported that they expect their federal partners to provide usable, timely, and actionable cyber threat information and alerts and other related services. However, according to private sector stakeholders, federal partners are not consistently meeting these expectations, despite improvement efforts, such as developing new information-sharing arrangements and expanding the number of private sector individuals with security clearances.

[18]For our most recent high risk report, see GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

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

Private Sector Stakeholders Expect Usable Threat and Alert Information and Other Related Services

Private sector stakeholders reported that they expect their federal partners to provide usable, timely, and actionable cyber threat information and alerts, access to sensitive or classified information, a secure mechanism for sharing information, security clearances, and a single centralized government cybersecurity organization to coordinate federal efforts. Some other services were less important, such as penetration testing of networks and financial support. Table 4 summarizes the extent to which the 56 private sector survey respondents expect to receive certain services from the federal government in order of most to least expected.

Table 4: Key Private Sector Expected Services Based on Survey Results

Services	Great or moderate extent
Timely and actionable cyber threat information	98%
Timely and actionable cyber alerts	96
Access to actionable classified or sensitive information (such as intelligence and law enforcement information)	87
A secure information-sharing mechanism	78
Security clearances	74
Quick response to recommendations to improve partnership	69
Participating in and obtaining results from exercises and simulations	59
Collaboration with international organizations	49
Development of exercise and simulation plans	44
Technical expertise	35
Training and workforce development opportunities	31
Assistance conducting vulnerability assessments	30
Policy expertise	29
Financial support	26
Penetration testing of networks	25%

Source: GAO analysis based on survey data of 56 private sector respondents.

The two most expected services private sector stakeholders want from their federal partners are timely and actionable cyber threat and alert information—providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. The percentages of private sector survey respondents reporting that they expect timely and actionable cyber threat and alert information to a great or moderate extent were 98 and 96, respectively. Private sector council representatives stated that they expect their federal partners to provide

timely and actionable intelligence on cyber-related issues that they can share within their membership. For example, one private sector official told us that time is of the essence when passing information to their members and that sector members expect to get a response within minutes so they can take appropriate actions as soon as possible.

Private sector stakeholders also identified access to sensitive government information, a secure information-sharing mechanism, and obtaining security clearances as key expectations. The percentages of survey respondents reporting that they expect these services to a great or moderate extent were 87, 78, and 74, respectively. Private sector officials stated that they need access to greater amounts of sensitive and classified government information. However, a private sector official indicated that access to classified information is not valuable because it can not be shared. This official stated that they would prefer information that is unclassified and actionable that can be shared. A private sector council member stated that their federal partners take too long to vet sensitive cyber information before private sector partners can receive and share it.

In addition, private sector officials and cyber experts stated that having a single or centralized government source for cyber-related information is important to (1) avoid confusion about who is the authoritative source, (2) have a consistent message communicated, and (3) coordinate a national response. Similarly, in March 2009, we testified that a panel of cyber security experts identified that creating an accountable, operational cybersecurity organization would be essential to improving our national cybersecurity posture.[20] The experts told us that there needs to be an independent cybersecurity organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, the military, the intelligence community, and the nation's international allies to address incidents against the nation's critical cyber systems and functions.

Conversely, private sector survey respondents stated that they expect some services to a lesser extent from their federal partners, including policy expertise, financial support, and penetration testing of their networks. The percentages of survey respondents reporting that they expect these services to a great or moderate extent were only 29, 26, and 25, respectively. In addition, government officials stated that having the

[20]GAO-09-432T.

government perform penetration testing could be construed as inappropriate by private entities and their customers whose information is stored on those systems.

Private Sector Stakeholders Believe That Critical Expectations Are Not Being Fully Met, Despite Federal Efforts

Federal partners are not consistently meeting private sector expectations, including providing timely and actionable cyber threat information and alerts, according to private sector stakeholders. Table 5 illustrates the degree to which the 56 private sector survey respondents reported that they are receiving services from the public sector in order of most to least expected. For example, only 27 percent of private sector survey respondents reported that they were receiving timely and actionable cyber threat information and alerts to a great or moderate extent. In addition, ISAC officials stated that the federal partners are not providing enough cyber threat information that is tailored to their sector's needs or analytical alert information that provides the tactics and techniques being used by cyber threats. According to these ISAC officials, this more specific information is needed to understand what actions will likely protect their networks. Another private sector council official said that a lot of the information they receive does not have enough detail to be useful.

Table 5: Private Sector Respondent Views on the Extent to Which Federal Partners Are Providing Expected Services

Services	Greatly or moderately provided
Timely and actionable cyber threat information	27%
Timely and actionable cyber alerts	27
Access to actionable classified or sensitive information (such as intelligence and law enforcement information)	16
A secure information-sharing mechanism	21
Security clearances	33
Quick response to recommendations to improve partnership	10
Participating in and obtaining results from exercises and simulations	18
Collaboration with international organizations	5
Development of exercise and simulation plans	34
Technical expertise	9
Training and workforce development opportunities	9
Assistance conducting vulnerability assessments	9
Policy expertise	25

Services	Greatly or moderately provided
Financial support	0
Penetration testing of networks	7%

Source: GAO analysis based on survey data of 56 private sector respondents.

Private sector stakeholders also reported a lack of access to classified information, a secure information-sharing mechanism, security clearances, and a single centralized government cyber-information source. Private sector survey respondents reported receiving access to actionable classified information, having access to a secure information sharing mechanism, and having adequate security clearances to a great or moderate extent at only 16, 21, and 33 percent, respectively. The private sector councils reported that they are not getting classified intelligence information that they perceive as being valuable to their efforts to defend their cyber resources from sophisticated attacks and that they do not have enough members with security clearances to receive classified information. Regarding the lack of a centralized source, an ISAC official stated that too many Internet-based information-sharing portals exist in the current cyber-related, public-private partnership and that the partnership could benefit from a "one-stop" portal. Another official suggested that one federal agency should be the clearing house for information and assigning tasks because there are too many government agencies working independently with their own unique missions. Further, a sector council official stated that there is too much duplication of projects and that it is not uncommon to work with six different groups doing almost the same thing and that these groups are not always aware of each other.

Federal partners are not meeting private sector stakeholders' expectations, in part, because of restrictions on the type of information that can be shared with the private sector. According to DHS officials, US-CERT's ability to provide information is impacted by restrictions that do not allow individualized treatment of one private sector entity over another private sector entity—making it difficult to formally share specific information with entities that are being directly impacted by a cyber threat. In addition, because US-CERT serves as the nation's cyber analysis and warning center, it must ensure that its warnings are accurate. Therefore, US-CERT's products are subjected to a stringent review and revision process that can adversely affect the timeliness of its products—potentially adding days to the release if classified or law enforcement information must be removed from the product. In addition, federal

officials are restricted to sharing classified information with only cleared private sector officials. Federal officials are also hesitant to share sensitive information with private sector stakeholders, in part, due to the fear that sensitive information shared with corporations could be shared openly on a global basis. By contrast, DOE officials stated that they are willing to share sensitive information with their energy sector member entities due to the long-standing nature of their relationships with the sector and the type of information being shared. In addition, according to federal officials, the limited number of private sector personnel with national security clearances makes it difficult to share classified information.

Another issue having an adverse affect on the federal partners' ability to meet private sector expectations is that federal officials do not have an adequate understanding of the specific private sector information requirements. Multiple private sector officials stated that federal partners could improve their methods of acquiring the type of information needed by the private sector. For example, more specific threat information would be focused on the technology being used by a particular entity or specify that a threat intends to target a particular entity, rather than including just broad threat information and alerts. In addition, this more specific information would focus on the specific needs for each sector rather than all of the sectors getting the same information. A private sector official also stated that the federal government often approaches the private sector on issues that are not a priority to the private sector but are issues the federal government thinks the private sector is interested in. Further, a cyber expert suggested that the partnership can improve if the government articulates what it needs from the private sector and assists the critical infrastructure sectors in understanding the direct benefit of their participation.

DOD and DHS have started pilot programs that are intended to improve the sharing of timely, actionable, and sensitive information with their private sector partners. Specifically, DOD's Defense Critical Infrastructure Program has a pilot program with some of its private sector DIB contractors to improve sharing of information on cyber threat, alerts, and sensitive data by establishing a new partnership model. This new program is known as the DIB Cyber Security/Information Assurance Program and is to facilitate the sharing of sensitive cyber information between the public and private sector. According to an agency official, this program involves a voluntary agreement between DOD and cleared DIB partners. DOD shares classified and unclassified cyber threat information and best practices. In return, the private sector partners agree to share cyber intrusion information with the DOD Cyber Crime Center, which is to serve as the

focal point for information-sharing and digital forensics analysis activities related to protecting unclassified information on DIB information systems and networks. DOD's goal is to transition from pilot to program status and expand the program to all qualified cleared contractors. In addition, the officials stated that they expect to eventually modify DOD contractual language to encourage contractors to increase cybersecurity in their networks.

In addition, DHS, in conjunction with DOD and the financial services sector, has developed an information sharing pilot program which began in December 2009. To date, this program has resulted in the federal government sharing 494 of its products, including sensitive information, with the Financial Services ISAC, and the Financial Services ISAC sharing 135 of its products with the government. According to DHS officials, DHS and the Financial Services ISAC are sharing sensitive information they did not share before the agreement. Both of these pilot programs are intended to improve federal partners' ability to share information over a secure mechanism. For example, DHS is using its US-CERT portal, and DOD is developing a DIB Net to communicate with its partners.

DHS and DOE have initiatives that specifically address sharing classified information with their partners. DHS officials stated that DHS has a process for clearing individual sector officials at the top secret and sensitive compartmented information levels. Further, in November 2009, DHS issued the Cybersecurity Partner Local Access Plan to improve the sharing of sensitive information between the public and private sectors. According to DOE officials, DOE also has an effort under way to increase the number of private officials from the energy sector with security clearances.

DHS has recently developed an integration center known as the National Cybersecurity and Communications Integration Center that is composed of the US-CERT and the National Coordinating Center for Telecommunications. This center is to provide a central place for the various federal and private-sector organizations to coordinate efforts to address cyber threats and to respond to cyber attacks. However, this center was only established in October 2009, is still in development, and does not currently have representation from all relevant federal agencies and private entities as envisioned. In addition, DHS officials stated that

they have taken steps to improve US-CERT's cyber analysis and warning capabilities in response to our previous recommendations.[21]

While the ongoing efforts may address the public sector's ability to meet the private sector's expectations, much work remains, and it is unclear if the efforts will focus on fulfilling the private sector's most expected services related to information-sharing. If the government does not improve its ability to meet the private sector's expectations, the partnerships will remain less than optimal, and the private sector stakeholders may not have the appropriate information and mechanisms needed to thwart sophisticated cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure.

Public Sector Stakeholders Expect Threat Information and Commitment, Which the Private Sector Is Generally Providing

Public sector stakeholders reported that they expect the private sector to provide a commitment to execute plans and recommendations, timely and actionable cyber threat information, and appropriate staff and resources. Four of the five government councils reported that the private sector is committed to executing plans and recommendations and providing timely and actionable threat information to a "great" or "moderate" extent. However, government council officials stated that improvements could be made to the partnership.

Public Sector Stakeholders Expect Usable Threat Information, Commitment, and Appropriate Staff and Resources

Public sector stakeholders reported that they expect a commitment to execute plans and recommendations, timely and actionable cyber threat information, and appropriate staff and resources to be provided by private sector stakeholders. All five government councils we met with stated that they expected these services from their private sector partners to a "great" or "moderate" extent.

Further, most government council representatives stated that they expect better communications and increasing trust between them and their private sector counterparts. For example, they would like the private sector to develop a strong dialogue with the government and keep the government informed about suspicious activities on private sector networks. Table 6 shows the government councils' expected services.

[21] GAO-08-588.

Table 6: Key Government Coordinating Councils' Expected Services from the Private Sector

	Public sectors				
Services	**Banking and finance**	**Communications**	**DIB**	**Energy**	**IT**
Commitment to execute plans and recommendations, such as best practices	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Great/moderate
Timely and actionable cyber threat information	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Great/moderate
Provide appropriate staff and resources	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Great/moderate
Timely and actionable cyber alerts	Some	Great/moderate	Great/moderate	Great/moderate	Great/moderate
Technical expertise	Great/moderate	Great/moderate	Great/moderate	Some	Great/moderate
Participation in and planning for exercises and simulation	Some	Great/moderate	Great/moderate	Great/moderate	Great/moderate
Quick response to recommendations to improve partnership	Great/moderate	Great/moderate	Great/moderate	Don't know	Great/moderate
Permission to conduct vulnerability assessments	Some	Great/moderate	Great/moderate	Some	Some
Collaboration with international organizations	Some	Great/moderate	Some	Great/moderate	Great/moderate
Permission to conduct penetration testing of networks	Some	Great/moderate	Don't know	Some	Some

Source: GAO analysis of agency data.

Private Sector Is Primarily Meeting Several Public Sector Expectations, but Some Gaps Exist

While many government councils reported that the private sector is mostly meeting their expectations in several areas, they also reported that improvements could be made. Four of the five government councils stated that they are receiving commitment to execute plans and recommendations and timely and actionable cyber threat information to a great or moderate extent. However, only two of the five government councils reported that the private sector is providing appropriate staff and resources. In addition, the extent to which the private sector is fulfilling the public sector's expectations varies by sector. Of the five councils, the communications government council reported most positively on whether the private sector was providing expected services. Specifically, it reported that its private sector partners were providing 8 of 10 expected services to a great or moderate extent. By contrast, the IT sector council reported that the private sector was providing only 1 of 10 expected services to a great or moderate extent and 5 of 10 expected services to

only some extent. Table 7 shows the extent to which the private sector is providing government councils' expected services.

Table 7: Extent to Which the Private Sector Is Providing the Government Coordinating Councils' Expected Services

	Public sectors				
Services	**Banking and finance**	**Communications**	**DIB**	**Energy**	**IT**
Commitment to execute plans and recommendations, such as best practices	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Little/no
Timely and actionable cyber threat information	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Some
Provide appropriate staff and resources	Great/moderate	Great/moderate	Some	Some	Some
Timely and actionable cyber alerts	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Some
Technical expertise	Great/moderate	Great/moderate	Great/moderate	Some	Great/moderate
Participation in and planning for exercises and simulation	Some	Great/moderate	Great/moderate	Great/moderate	Some
Quick response to recommendations to improve partnership	Great/moderate	Great/moderate	Great/moderate	Great/moderate	Little/no
Permission to conduct vulnerability assessments	Some	Some	Some	Some	Some
Collaboration with international organizations	Some	Great/moderate	Little/no	Some	Little/no
Permission to conduct penetration testing of networks	Little/no	Some	Don't know	Some	Little/no

Source: GAO analysis of agency data.

Although, in general, the private sector is meeting the expectations of the federal partners, there are still improvements that can be made. For example, while the government coordinating councils reported receiving timely and actionable cyber threat and alert information from the private sector, there are limits to the depth and specificity of the information provided, according to federal officials. One issue is that private sector stakeholders do not want to share their sensitive, proprietary information with the federal government. In addition, information security companies could lose a competitive advantage by sharing information with the government which, in turn, could share it with those companies' competitors. In addition, according to DHS officials, despite special protections and sanitization processes, private sector stakeholders are unwilling to agree to all of the terms that the federal government or a government agency requires to share certain information. Further, in some

cases, the lack of private sector commitment has had an adverse affect on the partnership.

Conclusions

The private-public partnership remains a key part of our nation's efforts to secure and protect its critical cyber-reliant infrastructure. For more than a decade, this private-public partnership has been evolving. While both private and public sector stakeholders report finding value in the partnership, the degree to which expectations are being met varies. Private sector stakeholders expect their federal partners to consistently provide usable, timely, actionable cyber threat information and alerts and, to a lesser extent, other related services. However, private sector stakeholders are not consistently receiving their expected services from their federal partners because, in part, federal partners are restricted in the type of information that can be shared with the private sector and lack an understanding about each sector's specific information requirements. In addition, many private sector stakeholders interact with multiple federal entities and multiple information sources, which can result in duplication of efforts and inconsistent information being shared.

In turn, federal partners primarily expect their private sector partners to provide commitment to execute plans and recommendations, timely and actionable cyber threat and alert information, and appropriate staff and resources, which the private sector is primarily providing; however, while most federal partners stated that these expectations are mostly being met, they identified difficulties with the private sector sharing their sensitive information and the need for private sector partners to improve their willingness to engage and provide support to partnership efforts. Federal and private sector partners have initiated efforts to improve the partnerships; however, much work remains to fully implement improved information sharing. Without improvements in meeting private and public sector expectations, the partnerships will remain less than optimal, and there is a risk that owners of critical infrastructure will not have the appropriate information and mechanisms to thwart sophisticated cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure.

Recommendations for Executive Action

We recommend that the Special Assistant to the President and Cybersecurity Coordinator and the Secretary of Homeland Security, in collaboration with the sector lead agencies, coordinating councils, and the owners and operators of the associated five critical infrastructure sectors, take two actions: (1) use the results of this report to focus their

information-sharing efforts, including their relevant pilot projects, on the most desired services, including providing timely and actionable threat and alert information, access to sensitive or classified information, a secure mechanism for sharing information, and providing security clearance and (2) bolster the efforts to build out the National Cybersecurity and Communications Integration Center as the central focal point for leveraging and integrating the capabilities of the private sector, civilian government, law enforcement, the military, and the intelligence community.

We are not making new recommendations regarding cyber-related analysis and warning at this time because our previous recommendations directed to DHS, the central focal point for such activity, in these areas have not yet been fully implemented.

Agency Comments and Our Evaluation

The national Cybersecurity Coordinator provided no comments on a draft of our report. DHS provided written comments on a draft of the report (see app. II), signed by DHS's Director of the Departmental GAO/OIG Liaison Office. In its comments, DHS concurred with our recommendations and described steps underway to address them. Regarding our first recommendation, DHS provided an additional example of and further detail about several pilot programs it has initiated to enable the mutual sharing of cybersecurity information at various classification levels. In addition, regarding our second recommendation, DHS stated that it is integrating government components and private sector partners into its National Cybersecurity and Communications Integration Center.

DHS also provided general comments. First, DHS noted that it is important to distinguish between actionable information and classified, contextual threat information. Specifically, DHS stated that sharing classified information with the private sector can pose a risk to national security and, consequently, such information is generally non-actionable. While we found that the private-sector stakeholders we surveyed and interviewed expect such information, we do not state that the federal government should share classified information with uncleared individuals. We distinguish in this report between sharing timely and actionable threat and alert information and providing access to classified information. In addition, we discuss US-CERT's review and revision process and identify DHS, DOD, and DOE efforts to provide clearances to private sector partners in order to share such information.

Second, DHS stated that the report makes generalizations about private-sector stakeholders which could be seen to suggest that such views were held across the entire cross-sector community. We acknowledge that our findings cannot be generalized across the sectors and clearly articulate that the scope of our review is limited to representatives from five critical infrastructure sectors.

Third, DHS also stated that the report focuses on surveyed participants "expectations," while the survey itself focused on "needs." DHS further stated that these two terms are not interchangeable for the concept of information sharing. During our review, we held numerous structured interviews with private and government stakeholders and surveyed private-sector stakeholders and asked separate questions on their expectations and needs. We acknowledge that the terms are not interchangeable and therefore appropriately reported on and distinguished both private and public sectors' expectations and needs.

Finally, DHS provided comments on the progress it has made in its sector planning approach and its clearance process.

DHS and DOD also provided technical comments, which we incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the national Cybersecurity Coordinator, the Secretary of Homeland Security, and other interested parties. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact me at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

David A. Powner
Director, Information Technology Management Issues

List of Congressional Requesters

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland security
House of Representatives

The Honorable Yvette D. Clarke
Chairwoman
Subcommittee on Emerging Threats, Cybersecurity,
and Science and Technology
Committee on Homeland Security
House of Representatives

The Honorable Shelia Jackson-Lee
Chairwoman
Subcommittee on Transportation Security
and Infrastructure Protection
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) public sector stakeholders' expectations for cyber-related public-private partnerships and to what extent expectations are being met. We focused our efforts on five critical infrastructure sectors: Communications, Defense Industrial Base, Energy, Banking and Finance, and Information Technology. We selected these five sectors because of their extensive reliance on cyber-based assets to support their operations. This determination was based on our analysis and interviews with cybersecurity experts and agency officials. Our findings and conclusions are based on information gathered from the five cyber-reliant critical sectors and are not generalizable to a larger population.

To determine private sector stakeholders' expectations for cyber-related public-private partnerships and to what extent these expectations are being met, we collected and analyzed various government and private sector reports and conducted structured interviews with sector coordinating councils representatives from the five critical infrastructure sectors. In addition, we interviewed additional experts in critical infrastructure protection from academia and information technology and security companies to gain a greater understanding of how the partnership should be working. We also interviewed representatives from the Communications, Electricity Sector, Financial Services, Information Technology, and Multi-State Information Sharing and Analysis Centers to understand their information-sharing needs. Finally, we conducted a survey of private sector representatives from the infrastructure sectors. The surveyed representatives were members of the information sharing and analysis centers, sector coordinating councils, associations within a sector, and/or owner/operators within a sector. These surveyed representatives were solicited by the leadership of those organizations to participate in our survey in order for them to fulfill their responsibility to protect the identity of their members. We administered the survey respondents' use of the electronic survey tool. We received 56 survey responses from across the five sectors. The survey results were used to determine the expectations of private sector stakeholders and the extent to which those expectations were being met.

To determine public sector stakeholders' expectations for cyber-related public-private partnerships and to what extent these expectations are being met, we collected and analyzed various government and private sector reports and conducted structured interviews with government coordinating councils representatives familiar with the cyber partnership

from the Banking and Finance, Communications, Defense Industrial Base, Energy, and Information Technology critical infrastructure sectors. We also met with representatives from DHS's National Cyber Security Division and Office of Infrastructure Protection to verify and understand the public sector's role in partnering with the private sector and encouraging the protection of the nation's cyber critical infrastructure.

We conducted this performance audit from June 2009 to July 2010 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.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 30, 2010

Mr. David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Powner:

RE: Draft Report GAO-10-628, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed* (Job Code 311205)

The Department of Homeland Security (Department/DHS) appreciates the opportunity to review and comment on the draft report referenced above. The Department, particularly the National Protection and Programs Directorate, agrees with the two recommendations contained therein.

Recommendation: The Special Assistant to the President and Cybersecurity Coordinator and the Secretary of Homeland Security, in collaboration with the other sector lead agencies, coordinating councils, and the owners and operators of the associated five critical infrastructure sectors use the results of this report to focus their information-sharing efforts, including their relevant pilot projects, on the most desired services, including providing timely and actionable threat and alert information, access to sensitive or classified information, a secure mechanism for sharing information, and providing security clearance.

Response: Concur. The Department agrees that more should be done to bolster public-private partnership and information sharing. As recommended, in collaboration with the Special Assistant to the President and Cybersecurity Coordinator, appropriate agencies, and private sector stakeholders, DHS will incorporate the applicable information from this report, as needed, in future action plans.

As we move forward, public-private cooperation is growing ever more important. We are building on already successful partnerships and looking forward to new opportunities. DHS is moving toward greater, more actionable sharing of information with the private sector based on new analytical insights derived from a comprehensive understanding of the government-wide cyber domain. DHS has initiated several pilot programs that enable the mutual sharing of cybersecurity information at various classification levels:

- DHS and Michigan are conducting a proof-of-concept pilot in which the EINSTEIN 1 network flow monitoring technology helps secure Michigan's dot-gov networks. The

- DHS and Michigan are conducting a proof-of-concept pilot in which the EINSTEIN 1 network flow monitoring technology helps secure Michigan's dot-gov networks. The purpose of this study is to help state governments enhance their cybersecurity and to increase DHS overall cyber situational awareness.

- DHS, the Department of Defense (DOD), and the Financial Services Information Sharing and Analysis Center have launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information—in both directions—to mitigate the impact of attempted cyber intrusions. This builds on the products and success of DOD's Defense Industrial Base initiative. This pilot is currently at the For Official Use Only level, but shortly will be enhanced to include Secret-level information.

- The Department is also working on a pilot that brings together state fusion centers and private sector owners and operators of critical infrastructure to provide access to Secret-level classified cybersecurity information. The Cybersecurity Partners Local Access Plan is a pilot initiative allowing security-cleared owners and operators of Critical Infrastructure and Key Resources (CIKR), as well as State Chief Information Security Officers and Chief Information Officers, to access Secret-level cybersecurity information and participate in Secret-level video teleconference calls via their local fusion centers, allowing classified information sharing outside of Washington, D.C.

- DHS has instituted a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance program for CIKR representatives to enable their engagement in analysis of the most sensitive cybersecurity threat information.

The Department also is working in the areas of software assurance and supply chain management so that government and private sector partners can work together to solve what is a potentially serious security issue. We believe software developers must automate security and institutionalize it from the beginning in an effort to change the current security posture from reactive to proactive.

Recommendation: The Special Assistant to the President and Cybersecurity Coordinator and the Secretary of Homeland Security, in collaboration with the other sector lead agencies, coordinating councils, and the owners and operators of the associated five critical infrastructure sectors bolster the efforts to build out the National Cybersecurity and Communications Integration Center as the central focal point for leveraging and integrating the capabilities of the private sector, civilian government, law enforcement, the military, and the intelligence community.

Response: Concur. The Department is currently completing phases I and II of operations for the National Cybersecurity and Communications Integration Center (NCCIC), which involves leveraging and integrating capabilities of the private sector, civilian government, law enforcement, the military, and the intelligence community. NCCIC is a 24-hour, DHS-led coordinated watch and warning center that should improve national efforts to address threats and

incidents affecting the nation's critical information technology and cyber infrastructure. Specifically, phases I and II, respectively, include the following:

- Integration of the government components -- National Coordinating Center for Telecommunications (NCC) and the United States Computer Emergency Readiness Team (US-CERT) -- brings together the most successful elements of its predecessors while adding greater efficiency, transparency, integration, and collaboration. This phase also includes functionally integrating elements of DHS's Office of Intelligence and Analysis and the National Cyber Security Center. Over time, all of these elements will be collocated in the new facility. Each organization will share information as authorized, build relationships, and work jointly when situations demand.

- Integration of private sector partners is critical to protect the nation's information technology and communication infrastructure. The NCC, the telecommunications operations center, already has a number of on-site private industry representatives from the communications sector. These representatives will be incorporated gradually and will maintain a similar working model until new standard operating procedures for handling steady-state and crisis operations are created and adopted by both industry and government. This includes industry representatives located within the watch and warning center who will interact with government counterparts to share relevant information. These actions and activities will facilitate timely and effective crisis operations in the event of a significant service disruption or cyber incident.

General Comments

Generally, it is important to distinguish between actionable information and classified, contextual threat information. The report does not clearly identify the difference. There appears to be a sense that the private sector could better secure its networks if it had access to actionable classified information. The difficulty is that sharing classified information in an open environment or with non-cleared personnel poses risk to national security. As such, classified information is generally non-actionable, and instead provides contextual threat information—focusing on the "who." This information needs to be shared with cleared private sector partners, and mechanisms are in place and being further developed to enable such sharing.

Actionable information, on the other hand, focuses on the "what" and the "how"—what is happening and how is the threat actor (whoever that actor may be) doing it? Public and private sector partners can better secure their networks and systems when provided with that information in a timely manner.

There are several instances where the draft report makes generalizations such as "according to private sector stakeholders" which presumes that the view is held across the entire cross-sector community when it was the response from surveyed representatives of five sectors. It would be more accurate to name specifically the actual source(s) of the statements.

The report focuses on surveyed participants' "expectations," when the survey itself focuses on "needs." The two terms are not interchangeable for the concept of information sharing.

GAO states that ". . . sector-specific agencies had yet to update their respective sector-specific plans to fully address key DHS cybersecurity criteria. The lack of complete updates and progress reports was further evidence that the sector planning process has not been effective, thus leaving the nation in the position of not knowing precisely where it stands in securing cyber critical infrastructures. Not following up to address these conditions also showed DHS was not making sector planning a priority. We recommended that DHS assess whether the existing sector-specific planning process should continue to be the nation's approach to securing cyber and other critical infrastructure and, if so, make the process an agency priority and implement it accordingly. DHS concurred with the recommendations."

The Department of Homeland Security supports the ongoing assessment and improvement of the sector planning approach. DHS continually assesses the effectiveness of this approach and identifies and implements improvements. The sector specific agencies have conducted a comprehensive triennial review and rewrite of their Sector Specific Plans (SSPs) which are due for reissue in 2010. DHS' guidance for the 2010 SSP rewrites is based on the updated 2009 NIPP and incorporates GAO's cyber criteria—criteria recommended by GAO during the GAO-08-113 audit. As DHS' sector-specific planning approach is based on a public-private partnership, DHS works with its partners to meet the intent of DHS guidance in a manner that addresses the unique characteristics and risks of their sector. This allows the (Sector Specific Agencies) SSAs to develop and implement appropriate programs and activities that specifically address their cyber security concerns; this approach allows the SSAs to work independently with their respective government and private sector coordinating councils and collaboratively with DHS to develop and implement Sector-Specific Plans that address sector needs. The 2010 Sector-Specific Plans are currently undergoing final reviews and will more fully reflect the integration of cyber considerations into the planning process, as appropriate to each sector.

The draft notes that "DHS officials stated that DHS is developing a process to clear individual sector officials at the TS/SCI levels." This process is already in place. Two CIKR sector representatives have already received their TS/SCI designations via the established process.

Again, we appreciate this opportunity to review and comment on the draft report. In addition to this response, technical comments have been provided under separate cover.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286, or pownerd@gao.gov

Staff Acknowledgments

In addition to the individual named above, Michael W. Gilmore, Assistant Director; Rebecca E. Eyler; Wilfred B. Holloway; Franklin D. Jackson; Barbarol J. James; Lee A. McCracken; Dana R. Pon; Carl M. Ramirez; Jerome T. Sandau; Adam Vodraska; and Eric D. Winter made key contributions to this report.