United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. (EDT)
Tuesday, September 16, 2008

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Better Address Its Cybersecurity Responsibilities

Statement of David Powner
Director, Information Technology Management Issues

September 16, 2008

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Better Address Its Cybersecurity Responsibilities

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1157T, a report to Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Recent cyber attacks demonstrate the potentially devastating impact these pose to our nation's computer systems and to the federal operations and critical infrastructures that they support. They also highlight that we need to be vigilant against individuals and groups with malicious intent, such as criminals, terrorists, and nation-states perpetuating these attacks. Federal law and policy established the Department of Homeland Security (DHS) as the focal point for coordinating cybersecurity, including making it responsible for protecting systems that support critical infrastructures, a practice commonly referred to as cyber critical infrastructure protection. Since 2005, GAO has reported on the responsibilities and progress DHS has made in its cybersecurity efforts. GAO was asked to summarize its key reports and their associated recommendations aimed at securing our nation's cyber critical infrastructure. To do so, GAO relied on previous reports, as well as two reports being released today, and analyzed information about the status of recommendations.

What GAO Recommends

GAO has previously made about 30 recommendations to help DHS fulfill its cybersecurity responsibilities and resolve underlying challenges. DHS in large part concurred with GAO's recommendations and in many cases has actions planned and underway to implement them.

To view the full product, including the scope and methodology, click on GAO-08-1157T. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

GAO has reported over the last several years that DHS has yet to fully satisfy its cybersecurity responsibilities. To address these shortfalls, GAO has made about 30 recommendations in the following key areas.

Key Cybersecurity Areas Reviewed by GAO
1. Bolstering cyber analysis and warning capabilities.
2. Reducing organizational inefficiencies.
3. Completing actions identified during cyber exercises.
4. Developing sector-specific plans that fully address all of the cyber-related criteria.
5. Improving cybersecurity of infrastructure control systems (which are computer-based systems that monitor and control sensitive processes and physical functions).
6. Strengthening DHS's ability to help recover from Internet disruptions.

Source: GAO analysis.

Specifically, examples of what GAO reported and recommended are as follows:

- Cyber analysis and warning—In July 2008, GAO reported that DHS's United States Computer Emergency Readiness Team (US-CERT) did not fully address 15 key cyber analysis and warning attributes. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. Consequently, GAO recommended that DHS address these attribute shortfalls.
- Cyber exercises—In September 2008, GAO reported that since conducting a cyber attack exercise in 2006, DHS demonstrated progress in addressing eight lessons it learned from this effort. However, its actions to address the lessons had not been fully implemented. GAO recommended that the department schedule and complete all identified corrective activities.
- Control systems—In a September 2007 report and October 2007 testimony, GAO identified that DHS was sponsoring multiple efforts to improve control system cybersecurity using vulnerability evaluation and response tools. However, the department had not established a strategy to coordinate this and other efforts across federal agencies and the private sector, and it did not effectively share control system vulnerabilities with others. Accordingly, GAO recommended that DHS develop a strategy to guide efforts for securing such systems and establish a process for sharing vulnerability information.

While DHS has developed and implemented capabilities to address aspects of these areas, it still has not fully satisfied any of them. Until these and other areas are effectively addressed, our nation's cyber critical infrastructure is at risk of increasing threats posed by terrorists, nation-states, and others.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing to discuss efforts in protecting our nation's critical infrastructures from cybersecurity threats. The recent computer-based, or cyber, attacks against nation-states and others demonstrate the potentially devastating impact these pose to systems and the operations and critical infrastructures that they support.[1] They also highlight the need to be vigilant against individuals and groups with malicious intent, such as criminals, terrorists, and nation-states perpetuating these attacks.

Today, I will discuss the Department of Homeland Security's (DHS) progress in fulfilling its responsibilities to protect systems that support critical infrastructures—a practice referred to as cyber critical infrastructure protection or cyber CIP—as well as its progress in addressing our related recommendations. 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 information technology systems security high-risk area in 2003 and have continued to report on its status since that time.[2]

As requested, my testimony will summarize our key reports—two of which are being released today at this hearing—and their associated recommendations aimed at securing our nation's cyber critical infrastructure. Specifically, these reports and recommendations focus on (1) providing cyber analysis and warning capabilities, (2) being effectively organized to plan for and respond to disruptions on

[1]Critical infrastructure is systems and assets, whether physical or virtual, so vital to the United States 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. There are 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.

[2]For our most recent high risk report, see GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

converged voice and data networks, (3) conducting and coordinating cyber attack exercises, (4) developing cyber-related sector-specific critical infrastructure plans, (5) securing control systems—computer-based systems that monitor and control sensitive processes and physical functions, and (6) coordinating public/private planning for Internet recovery from a major disruption.

In preparing for this testimony, we relied on our previous reports on department efforts to fulfilling its cyber CIP responsibilities. These reports contain detailed overviews of the scope and methodology we used. We also obtained and analyzed information about the implementation status of our recommendations. We conducted our work, in support of this testimony, from August 2008 through September 2008, in the Washington, D.C. area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results In Brief

Since 2005, we have reported that DHS has yet to fully satisfy its cybersecurity responsibilities. These reports included nearly 30 recommendations on key areas essential for DHS to address in order to fully implement its cybersecurity responsibilities. Examples of what GAO reported and recommended are as follows:

- **Cyber analysis and warning**—In a report being released today, we determined[3] that DHS's United States Computer Emergency Readiness Team (US-CERT) did not fully address 15 key cyber analysis and warning attributes related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US-CERT provided warnings by developing and

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

distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS agreed in large part with our recommendations.

- **Cyber exercises**—In another report[4] being issued today, we concluded that since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing eight lessons it learned from these efforts. However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the department identified 16 activities as ongoing and 7 as planned for the future. Consequently, we recommended that it schedule and complete all of the corrective activities identified so as to strengthen coordination between both public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation.

- **Control systems**—In a September 2007 report and October 2007 testimony,[5] we identified that DHS was sponsoring multiple control systems security initiatives, including efforts to (1) improve control systems cybersecurity using vulnerability evaluation and response tools and (2) build relationships with control systems vendors and infrastructure asset owners. However, DHS had not established a strategy to coordinate the various control systems activities across federal agencies and the private sector, and it did not effectively share information on control system vulnerabilities with the public and private sectors. Accordingly, we recommended that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control

[4]GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

[5]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08-119T (Washington, D.C.: Oct. 17, 2007).

system vulnerability information to improve federal government efforts to secure control systems governing critical infrastructure. DHS officials took our recommendations under advisement and more recently have begun developing a strategy, which is still a work in process. In addition, while DHS has begun developing a process to share sensitive information, it has not provided any evidence that the process has been implemented or that it is an effective information sharing mechanism.

Background

The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. In recent years, the sophistication and effectiveness of cyberattacks have steadily advanced.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and nation-states. As we reported[6] in June 2007, cybercrime has significant economic impacts and threatens U.S. national security interests. Various studies and experts estimate the direct economic impact from cybercrime to be in the billions of dollars annually. In addition, there is continued concern about the threat that our adversaries, including nation-states and terrorists, pose to our national security. For example, intelligence officials have stated that nation-states and terrorists could conduct a coordinated cyber attack to seriously disrupt electric power distribution, air traffic control, and financial sectors. In May 2007, Estonia was the reported target of a denial-of-service cyber attack

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

with national consequences. The coordinated attack created mass outages of its government and commercial Web sites.[7]

To address threats posed against the nation's computer-reliant infrastructures, federal law and policy establishes DHS as the focal point for cyber CIP. For example, within DHS, the Assistant Secretary of Cyber Security and Communications is responsible for being the focal point for national cyber CIP efforts. Under the Assistant Secretary is NCSD which interacts on a day-to-day basis with federal and nonfederal agencies and organizations (e.g., state and local governments, private-sector companies) regarding, among other things, cyber-related analysis, warning, information sharing, major incident response, and national-level recovery efforts. Consequently, DHS has multiple cybersecurity-related roles and responsibilities. In May 2005, we identified, and reported on, 13 key cybersecurity responsibilities called for in law and policy.[8] These responsibilities are described in appendix I.

Since then, we have performed detailed work and made recommendations on DHS's progress in fulfilling specific aspects of the responsibilities, as discussed in more detail later in this statement.

In addition to DHS efforts to fulfill its cybersecurity responsibilities, the President in January 2008 issued HSPD 23—also referred to as National Security Presidential Directive 54 and the President's "Cyber Initiative"—to improve DHS and the other federal agencies' cybersecurity efforts, including protecting against intrusion attempts and better anticipating future threats.[9] While the directive

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

[8]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO-05-434 (Washington, D.C.: May 26, 2005); *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005); and *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*. GAO-06-1087T (Washington, D.C.: Sept. 13, 2006).

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

has not been made public, DHS officials stated that the initiative includes steps to enhance cyber analysis related efforts, such as requiring federal agencies to implement a centralized network monitoring tool and reduce the number of connections to the Internet.

DHS Needs to Address Several Key Areas Associated with Its Cybersecurity Responsibilities

Over the last several years, we have reported that DHS has yet to comprehensively satisfy its key cybersecurity responsibilities. These reports included about 30 recommendations that we summarized into the following key areas that are essential for DHS to address in order to fully implement its cybersecurity responsibilities.

Table 1: Key Cybersecurity Areas Reviewed by GAO

1. Bolstering cyber analysis and warning capabilities.
2. Reducing organizational inefficiencies.
3. Completing actions identified during cyber exercises.
4. Developing sector-specific plans that fully address all of the cyber-related criteria.
5. Improving cybersecurity of infrastructure control systems.
6. Strengthening DHS's ability to help recover from Internet disruptions.

Source: GAO

Bolstering Cyber Analysis and Warning Capabilities

In July 2008, we identified[10] that cyber analysis and warning capabilities included (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. These four capabilities are comprised of 15 key attributes, which are detailed in appendix II.

[10]GAO-08-588.

We concluded that while US-CERT demonstrated aspects of each of the key attributes, it did not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtained information from numerous external information sources; however, it had not established a baseline of our nation's critical network assets and operations. In addition, while it investigated if identified anomalies constitute actual cyber threats or attacks as part of its analysis, it did not integrate its work into predictive analyses of broader implications or potential future attacks, nor does it have the analytical or technical resources to analyze multiple, simultaneous cyber incidents. The organization also provided warnings by developing and distributing a wide array of attack and other notifications; however, these notifications were not consistently actionable or timely—providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. Further, while it responded to a limited number of affected entities in their efforts to contain and mitigate an attack, recover from damages, and remediate vulnerabilities, the organization did not possess the resources to handle multiple events across the nation.

We also concluded that without the key attributes, US-CERT did not have the full complement of cyber analysis and warning capabilities essential to effectively perform its national mission. As a result, we made 10 recommendations to the department to address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS concurred with 9 of our 10 recommendations.

Reducing Organizational Inefficiencies

In June 2008, we reported[11] on the status of DHS's efforts to establish an integrated operations center that it agreed to adopt per recommendations from a DHS-commissioned expert task force. The two operations centers that were to be integrated were within the

[11]GAO, *Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruption on Converged Voice and Data Networks*, GAO-08-607 (Washington, D.C.: June 26, 2008).

department's National Communication System and National Cyber Security Division. We determined that DHS had taken the first of three steps towards integrating the operations centers—called the National Coordination Center Watch and US-CERT—it uses to plan for and monitor voice and data network disruptions. While DHS completed the first integration step by locating the two centers in adjacent space, it had yet to implement the remaining two steps. Specifically, although called for in the task force's recommendations, the department had not organizationally merged the two centers or involved key private sector critical infrastructure officials in the planning, monitoring, and other activities of the proposed joint operations center. In addition, the department lacked a strategic plan and related guidance that provides overall direction in this area and has not developed specific tasks and milestones for achieving the two remaining integration steps.

We concluded that until the two centers were fully integrated, DHS was at risk of being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that travel on this infrastructure, increasing the probability that communications will be unavailable or limited in times of need. As a result, we recommended that the department complete its strategic plan and define tasks and milestones for completing remaining integration steps so that we are better prepared to provide an integrated response to disruptions to the communications infrastructure. DHS concurred with our first recommendation and stated that it would address the second recommendation as part of finalizing its strategic plan.

DHS has recently made organizational changes to bolster its cybersecurity focus. For example, in response to the President's January 2008 Cyber Initiative, the department established a National Cybersecurity Center to ensure coordination among cyber-related efforts across the federal government. DHS placed the center at a higher organizational level than the Assistant Secretary of Cyber Security and Communications. As we previously reported,[12] this

[12] GAO-08-588.

placement raises questions about, and may in fact, diminish the Assistant Secretary's authority as the focal point for the federal government's cyber CIP efforts. It also raises similar questions about NCSD's role as the primary federal cyber analysis and warning organization.

Completing Corrective Actions Identified During A Cyber Exercise

In September 2008, we reported[13] on a 2006 major DHS-coordinated cyber attack exercise, called Cyber Storm, that included large scale simulations of multiple concurrent attacks involving the federal government, states, foreign governments, and private industry. We determined that DHS had identified eight lessons learned from this exercise, such as the need to improve interagency coordination groups and the exercise program. We also concluded that while DHS had demonstrated progress in addressing the lessons learned, more needed to be done. Specifically, while the department completed 42 of the 66 activities identified to address the lessons learned, it identified 16 activities as ongoing and 7 as planned for the future.[14] In addition, DHS provided no timetable for the completion dates of the ongoing activities. We noted that until DHS scheduled and completed its remaining activities, it was at risk of conducting subsequent exercises that repeated the lessons learned during the first exercise. Consequently, we recommended that DHS schedule and complete the identified corrective activities so that its cyber exercises can help both public and private sector participants coordinate their responses to significant cyber incidents. DHS agreed with the recommendation.

[13]GAO-08-825.

[14]DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

Developing Sector-Specific Plans That Fully Address All of the Cyber-Related Criteria

In 2007, we reported and testified[15] on the cybersecurity aspects of CIP plans for 17 critical infrastructure sectors, referred to as sector-specific plans. Specifically, we found that none of the plans fully addressed the 30 key cybersecurity-related criteria described in DHS guidance. We also determined that while several sectors' plans fully addressed many of the criteria, others were less comprehensive. In addition to the variations in the extent to which the plans covered aspects of cybersecurity, there was also variance among the plans in the extent to which certain criteria were addressed. For example, fewer than half of the plans fully addressed describing (1) a process to identify potential consequences of cyber attack or (2) any incentives used to encourage voluntary performance of risk assessments. We noted that without complete and comprehensive plans, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets. Consequently, we recommended[16] that DHS request that the lead federal agencies, referred to as sector-specific agencies, that are responsible for the development of CIP plans for their sectors fully address all cyber-related criteria by September 2008 so that stakeholders within the infrastructure sectors will effectively identify, prioritize, and protect the cyber aspects of their CIP efforts. The updated plans are due this month.

Improving Cybersecurity of Infrastructure Control Systems

In a September 2007 report and October 2007 testimony,[17] we identified that federal agencies had initiated efforts to improve the security of critical infrastructure control systems—computer-based systems that monitor and control sensitive processes and physical functions. For example, DHS was sponsoring multiple control

[15]GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-64T (Washington D.C.; October 31, 2007); and *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington D.C.; Oct. 31, 2007).

[16] GAO-08-113.

[17]GAO-07-1036 and GAO-08-119T.

systems security initiatives, including efforts to (1) improve control systems cybersecurity using vulnerability evaluation and response tools and (2) build relationships with control systems vendors and infrastructure asset owners. However, the department had not established a strategy to coordinate the various control systems activities across federal agencies and the private sector. Further, it lacked processes needed to address specific weaknesses in sharing information on control system vulnerabilities. We concluded that until public and private sector security efforts are coordinated by an overarching strategy and specific information sharing shortfalls are addressed, there was an increased risk that multiple organizations would conduct duplicative work and miss opportunities to fulfill their critical missions.

Consequently, we recommended[18] that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information to improve federal government efforts to secure control systems governing critical infrastructure. In response, DHS officials took our recommendations under advisement and more recently have begun developing a Federal Coordinating Strategy to Secure Control Systems, which is still a work in process. In addition, while DHS began developing a process to share sensitive information; it has not provided any evidence that the process has been implemented or that it is an effective information sharing mechanism.

Strengthening DHS's Ability to Help Recovery from Internet Disruptions

We reported and later testified[19] in 2006 that the department had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery. However, we determined that these efforts were not comprehensive

[18]GAO-07-1036.

[19]GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-06-863T (Washington, D.C.: July 28, 2006); and *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

or complete. As such, we recommended that DHS implement nine actions to improve the department's ability to facilitate public/private efforts to recover the Internet in case of a major disruption.

In October 2007, we testified[20] that the department had made progress in implementing our recommendations; however, seven of the nine have not been completed. For example, it revised key plans in coordination with private industry infrastructure stakeholders, coordinated various Internet recovery-related activities, and addressed key challenges to Internet recovery planning. However, it had not, among other things, finalized recovery plans and defined the interdependencies among DHS's various working groups and initiatives. In other words, it has not completed an integrated private/public plan for Internet recovery. As a result, we concluded that the nation lacked direction from the department on how to respond in such a contingency. We also noted that these incomplete efforts indicated DHS and the nation were not fully prepared to respond to a major Internet disruption.

- - - -

In summary, DHS has developed and implemented capabilities to satisfy aspects of key cybersecurity responsibilities. However, it still needs to take further action to fulfill all of these responsibilities. In particular, it needs to fully address the key areas identified in our recent reports. Specifically, it will have to bolster cyber analysis and warning capabilities, address organizational inefficiencies by integrating voice and data operations centers, enhance cyber exercises by completing the identified activities associated with the lessons learned, ensure that cyber-related sector-specific critical infrastructure plans are completed, improve efforts to address the cybersecurity of infrastructure control systems by completing a comprehensive strategy and ensuring adequate mechanisms for sharing sensitive information, and strengthen its ability to help recover from Internet disruptions by finalizing recovery plans and

[20]GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-08-212T (Washington, D.C.: Oct. 23, 2007).

defining interdependencies. Until these steps are taken, our nation's computer-reliant critical infrastructure remains at unnecessary risk of significant cyber incidents.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-9286, or by e-mail at pownerd@gao.gov. Other key contributors to this testimony include Michael Gilmore, Rebecca LaPaze, Kush Malhotra, and Gary Mountjoy.

Appendix I: DHS's Key Cybersecurity Responsibilities

Responsibilities	Description of responsibilities
Develop a national plan for CIP that includes cybersecurity	Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including information technology and telecommunications systems (including satellites) and the physical and technological assets that support such systems. This plan is to outline national strategies, activities, and milestones for protecting critical infrastructures.
Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector	Fostering and developing public/private partnerships with and among other federal agencies, state and local governments, the private sector, and others. DHS is to serve as the "focal point for the security of cyberspace."
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities	Improving and enhancing information sharing with and among other federal agencies, state and local governments, the private sector, and others through improved partnerships and collaboration, including encouraging information sharing and analysis mechanisms. DHS is to improve sharing of information on cyber attacks, threats, and vulnerabilities.
Develop and enhance national cyber analysis and warning capabilities	Providing cyber analysis and warnings, enhancing analytical capabilities, and developing a national indications and warnings architecture to identify precursors to attacks.
Provide and coordinate incident response and recovery planning efforts	Providing crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cybersecurity continuity plans for federal systems, planning for recovery of Internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans.
Identify and assess cyber threats and vulnerabilities	Leading efforts by the public and private sector to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies.
Support efforts to reduce cyber threats and vulnerabilities	Leading and supporting efforts by the public and private sector to reduce threats and vulnerabilities. Threat reduction involves working with the law enforcement community to investigate and prosecute cyberspace threats. Vulnerability reduction involves identifying and remediating vulnerabilities in existing software and systems.
Promote and support research and development efforts to strengthen cyberspace security	Collaborating and coordinating with members of academia, industry, and government to optimize cybersecurity-related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies.
Promote awareness and outreach	Establishing a comprehensive national awareness program to promote efforts to strengthen cybersecurity throughout government and the private sector, including the home user.
Foster training and certification	Improving cybersecurity-related education, training, and certification opportunities.
Enhance federal, state, and local government cybersecurity	Partnering with federal, state, and local governments in efforts to strengthen the cybersecurity of the nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States.
Strengthen international cyberspace security	Working in conjunction with other federal agencies, international organizations, and industry in efforts to promote strengthened cybersecurity on a global basis.
Integrate cybersecurity with national security	Coordinating and integrating applicable national preparedness goals with its National Infrastructure Protection Plan.

Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace.*

Appendix II: Key Attributes of Cyber Analysis and Warning Capabilities

Capability	Attribute
Monitoring	• Establish a baseline understanding of network assets and normal network traffic volume and flow • Assess risks to network assets • Obtain internal information on network operations via technical tools and user reports • Obtain external information on threats, vulnerabilities, and incidents through various relationships, alerts, and other sources • Detect anomalous activities
Analysis	• Verify that an anomaly is an incident (threat of attack or actual attack) • Investigate the incident to identify the type of cyber attack, estimate impact, and collect evidence • Identify possible actions to mitigate the impact of the incident • Integrate results into predictive analysis of broader implications or potential future attack
Warning	• Develop attack and other notifications that are targeted and actionable • Provide notifications in a timely manner • Distribute notifications using appropriate communications methods
Response	• Contain and mitigate the incident • Recover from damages and remediate vulnerabilities • Evaluate actions and incorporate lessons learned

Source: GAO analysis.