United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees
Committee on Homeland Security
U.S. House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, October 31, 2007

CRITICAL INFRASTRUCTURE PROTECTION

Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

Statement of David A. Powner
Director, Information Technology Management Issues

October 31, 2007

CRITICAL INFRASTRUCTURE PROTECTION

Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-64T, a testimony before congressional subcommittees, Committee on Homeland Security, U.S. House of Representatives

Why GAO Did This Study

The nation's critical infrastructure sectors—such as banking and finance, information technology, and public health—rely on computerized information and systems to provide services to the public. To fulfill the requirement for a comprehensive plan, including cyber aspects, the Department of Homeland Security (DHS) issued a national plan in June 2006 for the sectors to use as a road map to enhance the protection of critical infrastructure. Lead federal agencies, referred to as sector-specific agencies, are responsible for coordinating critical infrastructure protection efforts such as the development of plans that are specific to each sector. GAO was asked to summarize a report being released today that identifies the extent to which the sector plans addressed key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans. In the report, GAO analyzed each sector-specific plan against criteria that were developed on the basis of DHS guidance.

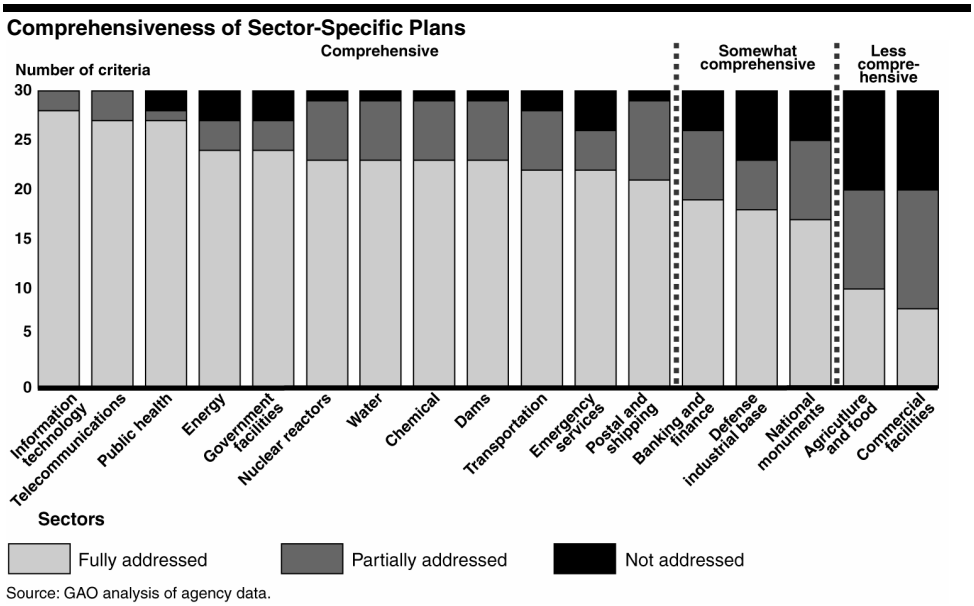
What GAO Recommends

In its report, GAO recommends that the Secretary of Homeland Security request that, by September 2008, the sector-specific agencies develop plans that fully address all of the cyber-related criteria. In written comments on a draft of the report, DHS concurred with GAO's recommendation.

To view the full product, including the scope and methodology, click on GAO-08-64T. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

The extent to which the sectors addressed aspects of cyber security in their sector-specific plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several sector plans—including the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as agriculture and food and commercial facilities—were less comprehensive. The following figure summarizes the extent to which each plan addressed the 30 criteria.



Source: GAO analysis of agency data.

In addition to the variations in the extent to which the plans covered aspects of cyber security, there was also variance among the plans in the extent to which certain criteria were addressed. For example, all plans fully addressed identifying a sector governance structure for research and development, but fewer than half of the plans fully addressed describing any incentives used to encourage voluntary performance of risk assessments. The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity in the different sectors.

DHS acknowledges the shortcomings in the plans. DHS officials stated that the sector-specific plans represent only the early efforts by the sectors to develop their respective plans. Nevertheless, until the plans fully address key cyber elements, certain sectors may not be prepared to respond to a cyber attack against our nation's critical infrastructure. As the plans are updated, it will be important that DHS work with the sector representatives to ensure that the areas not sufficiently addressed are covered. Otherwise, the plans will remain incomplete and sector efforts will not be sufficient to enhance the protection of their computer-reliant assets.

Mr. Chairman, Madame Chairwoman, and Members of the Subcommittees:

Thank you for the opportunity to join in today's hearing to discuss transitioning critical infrastructure protection sector-specific plans into action. Because the nation's critical infrastructure relies extensively on computerized information systems and electronic data to maintain the nation's security, economy, and public health and safety, the security of those systems and information is essential. To help address critical infrastructure protection, federal policy has established a framework for public- and private-sector partnerships.[1] It has also identified 17 critical infrastructure sectors that are largely owned and operated by the private sector, including banking and finance, information technology, telecommunications, energy, and public health and healthcare.

Federal policy requires the development of a national plan by the Department of Homeland Security (DHS) to outline national goals, objectives, milestones, and key initiatives as well as the development of individual critical infrastructure sector plans—referred to as sector-specific plans—to outline how a sector's public and private stakeholders will implement the national plan. Lead federal agencies, referred to as sector-specific agencies (including DHS, Department of the Treasury, and the Department of Health and Human Services), are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

DHS issued a National Infrastructure Protection Plan (NIPP) in June 2006 to be used as a road map for how DHS and other relevant stakeholders are to use risk management principles to prioritize protection activities within and across the sectors in an integrated, coordinated fashion. NIPP requires each of the lead federal agencies associated with the 17 critical infrastructure sectors to develop sector-specific plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets, systems, networks, and functions. These plans are to, among other things, describe how the sector will identify and prioritize its critical assets, including cyber assets, and define approaches the sector will take to assess risks and develop

[1]The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: Dec. 17, 2003). Department of Homeland Security, *National Infrastructure Protection Plan*, (Washington, D.C.: June 2006).

programs to protect those assets. DHS announced the release of the 17 sector plans on May 21, 2007.

As requested, our testimony today will summarize our report being released today on the cyber security aspects of the critical infrastructure protection sector-specific plans.[2] In the report, we analyzed each sector-specific plan against 30 criteria that we developed based on DHS guidance. The 30 criteria are shown in appendix I. The report contains a detailed overview of the scope and methodology we used. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

The extent to which the sectors addressed key aspects of cyber security in their sector-specific plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several plans—including those from the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as those from the agriculture and food and commercial facilities sectors—were not as comprehensive. In addition to the varying degrees with which the sector-specific plans covered aspects of cyber security, the plans as a whole addressed certain criteria more comprehensively than they did others. For example, all 17 plans fully addressed the criterion to identify a sector governance structure for research and development, while only 7 plans fully addressed the process for identifying the consequences of cyber attacks. Further, only 3 plans fully addressed the criterion to describe incentives used to encourage voluntary performance of risk assessments.

The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity of the different sectors: that is, sectors where stakeholders had more experience working together on critical infrastructure issues generally had more comprehensive and complete plans than those in which their stakeholders had less prior experience working together. Without comprehensive plans, certain sectors may not be effectively identifying, prioritizing, and protecting the cyber aspects of their critical infrastructure protection efforts. For example, with most sectors lacking a process for identifying the consequences of cyber attacks against their assets, our

[2]GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington, D.C.: Oct. 31, 2007).

nation's sectors could be ill-prepared to respond properly to a cyber attack.

To assist the sectors in securing their cyber infrastructure, we made a recommendation in our report to the Secretary of Homeland Security to request that by September 2008, the sector-specific agencies' plans address the cyber-related criteria that have not been fully addressed. In written comments on a draft of the report, DHS concurred with our recommendation.

Background

Our nation's critical infrastructures—such as banking and finance, information technology, telecommunications, energy, and public health and healthcare—rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data, referred to as cyber critical infrastructure protection, is essential to preventing disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Due in part to the importance of and increasing reliance on these electronic systems, we designated cyber critical infrastructure protection, in conjunction with protecting the federal government's information systems, as a high risk area in 2003. In January 2005 and 2007, we identified cyber critical infrastructure protection as a high-risk area because of the continuing concern about risks to information systems from escalating and emerging threats; the ease of obtaining and using hacking tools; the steady advance in the sophistication of attack technology; and the emergence of new and more destructive attacks.

As the focal point for critical infrastructure protection, DHS has many cyber security-related roles and responsibilities that are called for in law and policy. In May 2005, we identified 13 key cyber security responsibilities (see table 1).[3] These responsibilities are described in more detail in appendix II.

[3]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO-05-434 (Washington, D.C.: May 26, 2005).

Table 1: DHS Key Cyber Security Responsibilities

1.	Develop a comprehensive national plan for critical infrastructure protection, including cyber security.
2.	Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.
3.	Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.
4.	Develop and enhance national cyber analysis and warning capabilities.
5.	Provide and coordinate incident response and recovery planning efforts.
6.	Identify and assess cyber threats and vulnerabilities.
7.	Support efforts to reduce cyber threats and vulnerabilities.
8.	Promote and support research and development efforts to strengthen cyber space security.
9.	Promote awareness and outreach.
10.	Foster training and certification.
11.	Enhance federal, state, and local government cyber security.
12.	Strengthen international cyber space security.
13.	Integrate cyber security with national security.

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

In May 2005, we reported that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 responsibilities.[4] For example, the department established the United States Computer Emergency Readiness Team as a public/private partnership to make cyber security a coordinated national effort and it established forums to build greater trust and information sharing among federal officials who have information security responsibilities and law enforcement entities. However, DHS had not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cyber security. In September 2006, we testified that DHS had made progress on its responsibilities, but that none had been completely addressed.[5]

One of DHS's key cyber security responsibilities is the development of a comprehensive national plan for securing both the physical and cyber

[4]GAO-05-434.

[5]GAO, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*, GAO-06-1087T (Washington, D.C.: Sep. 13, 2006).

aspects of the key resources and critical infrastructure of the United States. The plan is to outline national strategies, activities, and milestones for protecting critical infrastructures. To fulfill this responsibility, in June 2006, DHS issued the National Infrastructure Protection Plan (NIPP) to guide how DHS and other relevant stakeholders are to use risk management principles to prioritize protection activities within and across the sectors in an integrated, coordinated fashion. NIPP requires each of the lead federal agencies associated with the 17 critical infrastructure sectors to develop sector-specific plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets, systems, networks, and functions. As part of these efforts, DHS provided guidance to the sectors for developing their sector-specific plans, including guidance on cyber aspects.

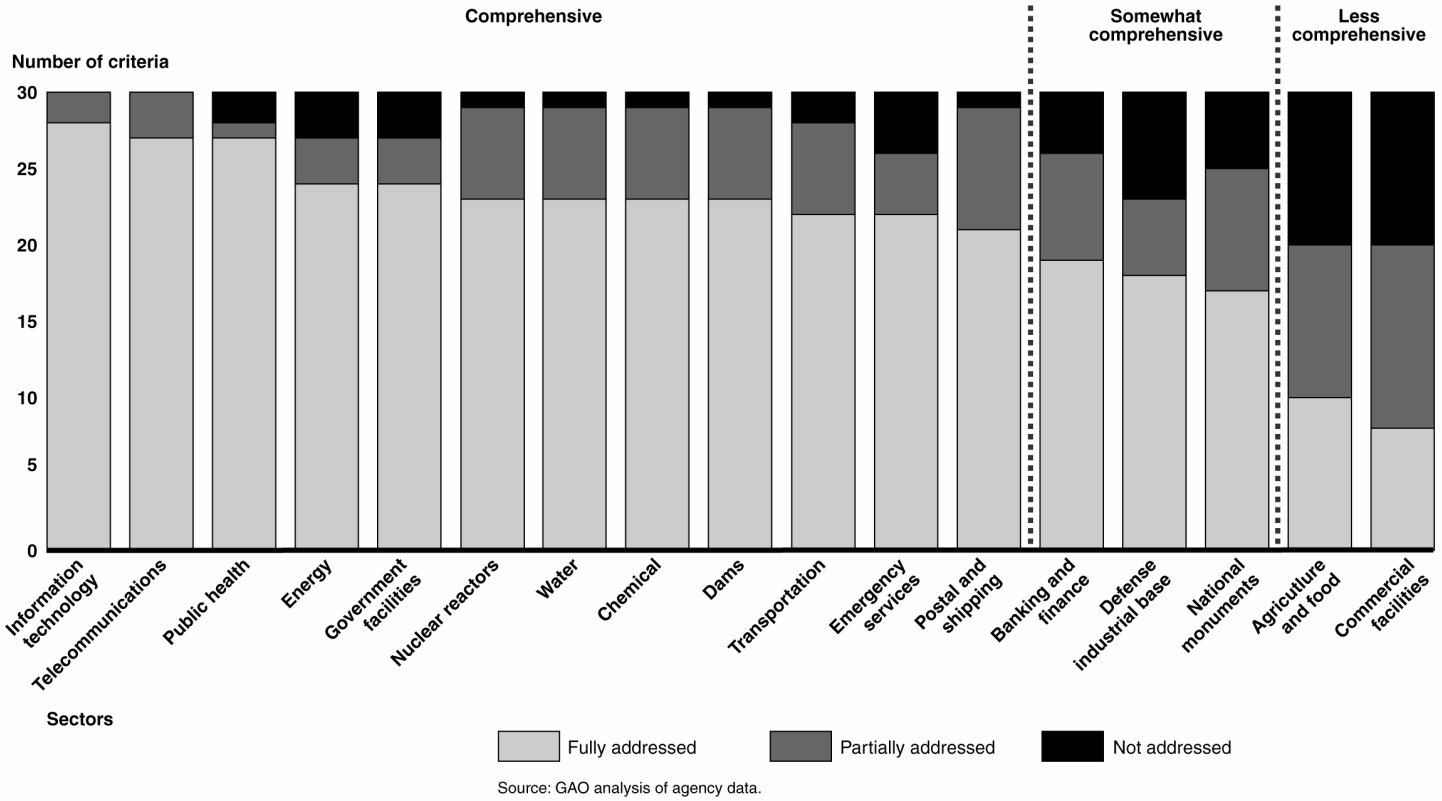
To strengthen DHS's ability to implement its cyber security responsibilities and to resolve underlying challenges, we have made about 25 recommendations over the last several years. These recommendations focus on the need to (1) conduct threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption. For example, in May 2005, we recommended, among other things, that DHS prioritize key cyber security responsibilities, including: performing a national cyber threat assessment and facilitating sector cyber vulnerability assessments. DHS has made varying levels of progress on many of these recommendations; however, additional efforts are needed to fully address them. Regarding the protection of infrastructure control systems, we issued a report on September 10, 2007, and testified on October 17, 2007, before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, House Committee on Homeland Security. In the report, we made a recommendation that DHS develop a strategy for coordinating control systems security efforts and enhance information sharing with control systems stakeholders.[6] Collectively, our recommendations provide a high-level road map for the agency to use in improving our nation's cyber security posture.

[6]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but More Remains to Be Done*, 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).

Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

In May 2007, DHS announced the release of 17 sector-specific plans to fulfill the NIPP requirement for individual sector plans. The extent to which the sectors addressed aspects of cyber security in their plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several plans—including those from the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as agriculture and food and commercial facilities—were less comprehensive. Figure 1 summarizes the extent to which each plan addressed the 30 criteria.

Figure 1: Comprehensiveness of Sector-Specific Plans



Source: GAO analysis of agency data.

In addition to the variations in the extent to which the plans covered aspects of cyber security, there was also variance among the plans in the extent to which certain criteria were addressed. For example, all plans fully addressed (1) identifying a sector governance structure for research and development, (2) describing how the sector-specific agency intends to manage its NIPP responsibilities; and (3) describing the sector's

coordinating mechanisms and structures. Also, at least 15 of the plans fully addressed (1) characterizing the sector's infrastructure, including the cyber reliance, (2) identifying stakeholder relationships for securing cyber assets, (3) describing a process for updating, reporting, budgeting, and training, and (4) describing a process for cyber-related information sharing. However, fewer than half of the plans fully addressed: (1) describing a process to identify potential consequences of cyber attacks, (2) describing any incentives used to encourage voluntary performance of risk assessments, (3) developing and using cyber metrics to measure progress, and (4) identifying existing cyber-related projects that support goals and identify gaps.

The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity of the different sectors. According to DHS officials, the sectors that have been working together longer on critical infrastructure issues generally have developed more comprehensive and complete plans than the sectors with stakeholders that had not previously worked together. For example, the plan for the energy sector was among those categorized as most comprehensive: the chemical sector had worked with DHS to improve the cyber component in its plans and it included most of the key information required for each plan element. Furthermore, the limited amount of time to complete the plans—6 months—was a factor for those sectors that had not previously been working together on critical infrastructure issues and were thus less mature.

DHS acknowledges the shortcomings we identified in the plans. Officials stated that the sector-specific plans represent only the early efforts by the sectors to develop their respective plans and anticipate that the plans will improve over time. Nevertheless, until the plans fully address key cyber elements, certain sectors may not be prepared to respond to a cyber attack against our critical infrastructure. As the plans are updated, it will be important that DHS work with the sector representatives to ensure that the areas not sufficiently addressed are covered. Otherwise, the plans will remain incomplete and sector efforts will not be sufficient to enhance the protection of their computer-reliant assets.

To assist the sectors in securing their cyber infrastructure, we recommended in our report that the Secretary of Homeland Security direct the Assistant Secretary for Infrastructure Protection and the Assistant Secretary for Cybersecurity and Communications to request that by September 2008, the sector-specific agencies' plans address the cyber-related criteria that were not fully addressed. In written comments on a

draft of the report, DHS's Director, Departmental GAO/OIG Liaison, concurred with our recommendation. In addition, he stated that DHS is currently working on an action plan to assist sectors in addressing cyber security issues not adequately addressed in the initial sector-specific plans.

In summary, without comprehensive plans, certain sectors may not be effectively identifying, prioritizing, and protecting the cyber aspects of their critical infrastructure. For example, with most sectors lacking a process for identifying the consequences of cyber attacks against their assets, our nation's sectors could be ill-prepared to respond properly to a cyber attack. In addition, without comprehensive plans, DHS cannot adequately identify where it and the rest of the federal government can most effectively assist in enhancing the security of the nation's critical infrastructures that are largely owned and operated by the private sector.

Ultimately, our nation needs to move beyond the planning stages of securing our critical infrastructures and public and private sector owners and operators of our nation's critical infrastructure need to effectively implement these plans. Implementation of these plans is more likely if DHS can successfully fulfill its role as a focal point for critical infrastructure protection. To accomplish this, DHS needs to address its 13 key responsibilities and our previous recommendations. For example, if DHS enhanced national cyber analysis and warning capabilities and provided assessments of cyber threats and vulnerabilities, it would be viewed as providing a valuable service to critical infrastructure owners, thus improving our nation's ability to prepare for, respond to, and prevent major cyber attacks from occurring.

Mr. Chairman and Madame Chairwoman, this concludes my statement. I would be happy to answer any questions 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 Scott Borre, Michael Gilmore, Nancy Glover, Barbarol James, and Eric Winter.

Appendix I: Cyber Security Criteria

Section 1: Sector Profile and Goals

- Characterizes cyber aspects
- Identifies stakeholder relationships for securing cyber assets

Section 2: Identify Assets, Systems, Networks, and Functions

- Describes process to identify cyber assets, functions, or elements
- Describes process to identify cyber dependencies/independences

Section 3: Assess Risks

- Describes how the risk assessment process addresses cyber elements
- Describes a screening process for cyber aspects
- Describes methodology to identify potential consequences of cyber attacks
- Describes methodology for vulnerability assessments of cyber aspects
- Describes methodology for threat analyses of cyber aspects
- Describes incentives to encourage voluntary vulnerability assessments

Section 4: Prioritizing Infrastructure

- Identifies entity responsible for prioritization of cyber aspects
- Describes criteria and basis for prioritization of cyber aspects

Section 5: Develop and Implement Protective Programs

- Describes process to develop long-term protective plans for cyber aspects
- Describes process to identify specific cyber-related program needs
- Identifies programs to deter, respond, and recover from cyber attack
- Addresses implementation and maintenance of protective programs

Section 6: Measure Progress

- Ensures that integration of cyber metrics is part of measurement process
- Describes how cyber metrics will be reported to DHS
- Includes developing and using cyber metrics to measure progress
- Describes how to use metrics to guide future cyber projects

Section 7: Critical Infrastructure Protection Research and Development

- Describes how technology developments are related to the sector's cyber goals
- Describes process to identify cyber security technology requirements
- Describes process to solicit information on ongoing cyber research and development initiatives
- Identifies existing cyber-related projects that support goals and identifies gaps
- Identifies research and development governance structure

Section 8: Managing Sector-Specific Agency Responsibilities

- Describes sector-specific agency's management of NIPP responsibilities
- Describes process for updating, reporting, budgeting, and training
- Describes sector's coordination structure
- Describes process for investment priorities
- Describes process for cyber-related information sharing

Source: GAO analysis based on DHS guidance.

Appendix II: Thirteen DHS Cyber Security Responsibilities

Critical infrastructure protection responsibilities with a cyber element	DHS responsibilities
1. Develop a national plan for critical infrastructure protection that includes cyber security	Develop 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.
2. Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector	Foster and develop 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 cyber space.
3. Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities	Improve and enhance 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.
Responsibilities related to the cyber space strategy's five priorities	
4. Develop and enhance national cyber analysis and warning capabilities	Provide cyber analysis and warnings, enhance analytical capabilities, and develop a national indications and warnings architecture to identify precursors to attacks.
5. Provide and coordinate incident response and recovery planning efforts	Provide crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cyber security continuity plans for federal systems, planning for recovery of Internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans.
6. Identify and assess cyber threats and vulnerabilities	Lead efforts by the public and private sectors to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies.
7. Support efforts to reduce cyber threats and vulnerabilities	Lead and support efforts by the public and private sectors 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.
8. Promote and support research and development efforts to strengthen cyber space security	Collaborate and coordinate with members of academia, industry, and government to optimize cyber security-related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies.
9. Promote awareness and outreach	Establish a comprehensive national awareness program to promote efforts to strengthen cyber security throughout government and the private sector, including the home user.
10. Foster training and certification	Improve cyber security-related education, training, and certification opportunities.
11. Enhance federal, state, and local government cyber security	Partner with federal, state, and local governments in efforts to strengthen the cyber security of the nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States.
12. Strengthen international cyberspace security	Work in conjunction with other federal agencies, international organizations, and industry in efforts to promote strengthened cyber security on a global basis.
13. Integrate cyber security with national security	Coordinate and integrate applicable national preparedness goals with the National Infrastructure Protection Plan.

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

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

Susan Becker, Acting Manager, BeckerS@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON RECYCLED PAPER