United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2007

CRITICAL INFRASTRUCTURE PROTECTION

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

GAO-08-113

October 2007

CRITICAL INFRASTRUCTURE PROTECTION

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

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-113, a report to congressional requesters

Why GAO Did This Study

The nation's critical infrastructure sectors—such as public health, energy, water, and transportation—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. In this context, GAO was asked to determine if these sector-specific plans address key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans. To accomplish this, GAO analyzed each sector-specific plan against criteria that were developed on the basis of DHS guidance.

What GAO Recommends

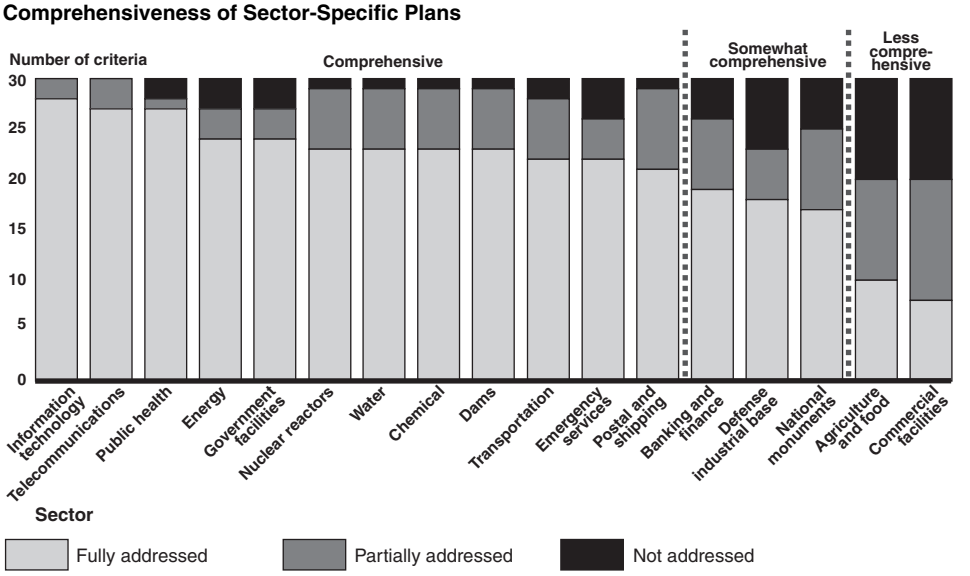
To assist the sectors in securing their cyber infrastructure, GAO recommends that the Secretary of Homeland Security request that, by September 2008, the sector-specific agencies develop plans that address all of the cyber-related criteria. In written comments on a draft of this report, DHS concurred with GAO's recommendation and provided technical comments that have been addressed as appropriate.

To view the full product, including the scope and methodology, click on GAO-08-113. 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.

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 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, and 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, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets. 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.

Contents

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 31, 2007

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats, Cybersecurity,
and Science and Technology
Committee on Homeland Security
House of Representatives

Because the nation's critical infrastructure relies extensively on computerized information systems and electronic data, the security of those systems and information is essential to our nation's security, economy, and public health and safety. To help address critical infrastructure protection, federal policy has established a framework for public and private sector partnerships and identified 17 critical infrastructure sectors, including banking and finance, information technology, telecommunications, energy, and public health and healthcare.[1]

The Department of Homeland Security (DHS) is a key player in these partnerships. The agency 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. Lead federal agencies, referred to as sector-specific agencies (including DHS, the Department of the Treasury, and the Department of Health and Human Services), are responsible for

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

coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

The NIPP requires each of the lead federal agencies associated with the 17 critical infrastructure sectors to develop 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 sector-specific 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 programs to protect these assets.

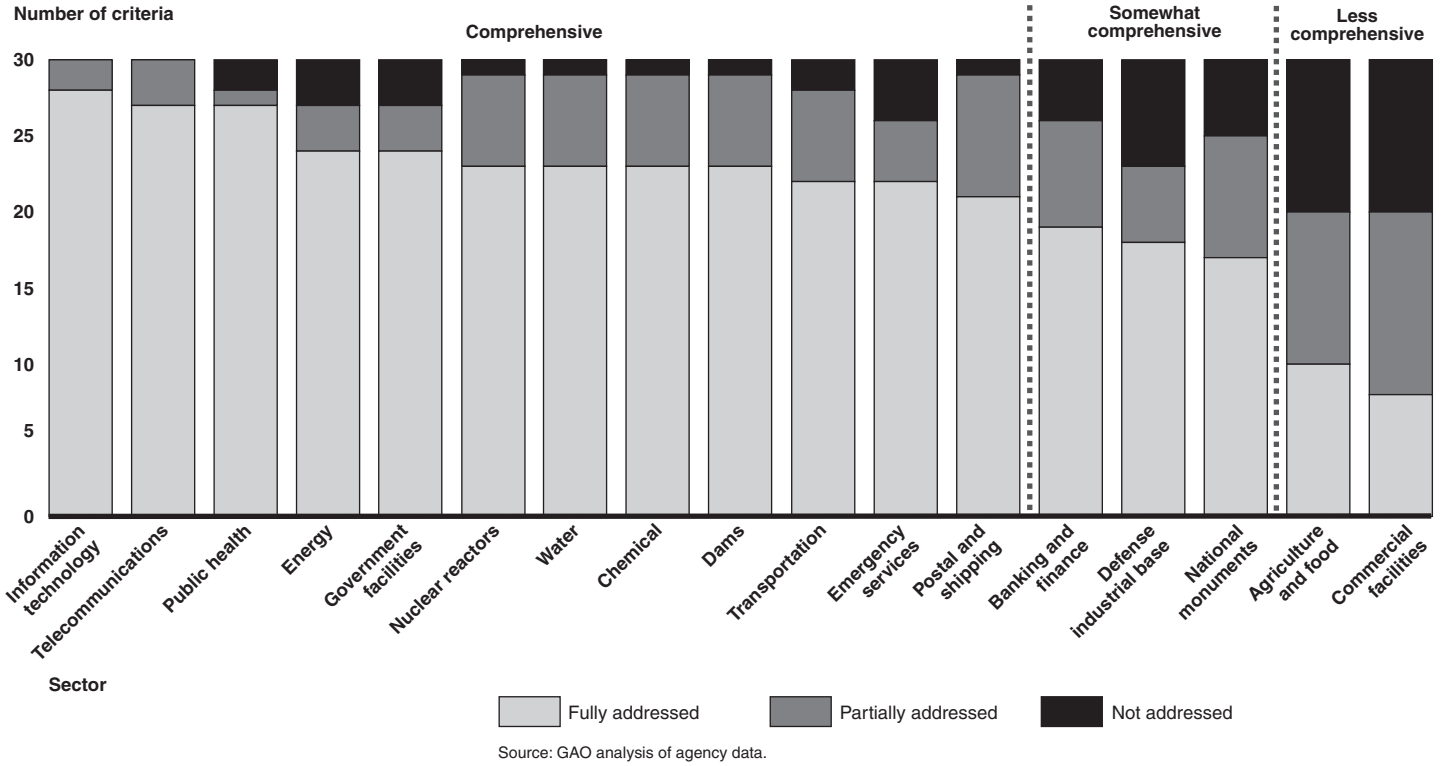
As agreed, our objective was to determine if the sector-specific plans address key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans. To accomplish this objective, we analyzed each sector-specific plan against 30 criteria that were developed on the basis of DHS guidance.

On August 7 and 20, 2007, we presented a briefing to the staffs of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs, respectively. This report transmits the presentation slides we used to brief the staffs and the recommendation that we made to the Secretary of Homeland Security. The full briefing, including our scope and methodology, is reprinted in appendix I. In commenting on a draft of this report, the Director, DHS Departmental GAO/OIG Liaison, concurred with our recommendation. In addition, DHS provided technical comments that have been addressed in this report as appropriate.

Compliance with Aspects of Cyber Security Criteria

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 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 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, while fewer than half of the plans fully addressed describing any incentives used to encourage voluntary performance of risk assessments.

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

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 included most of the key information required for each plan element, and the chemical sector had worked with DHS to improve the cyber component in its plans; this sector's plan was among those categorized as comprehensive. Furthermore, for those sectors that had not been previously working together on critical infrastructure issues and were thus less mature, the limited amount of time to complete the plans—6 months—was a factor in their plans being less comprehensive and complete.

DHS acknowledges the GAO-identified 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 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 nation's critical infrastructure.

Conclusions

The sector-specific plans varied in how comprehensively they addressed the cyber security aspects of their sectors. Without comprehensive plans, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets, systems, networks, and functions; be prepared to respond to a significant attack; or identify the cyber risks they face. 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 selected sectors' efforts will remain insufficient to enhance the protection of their computer-reliant assets.

Recommendation for Executive Action

To assist the sectors in securing their cyber infrastructure, we recommended 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 only partially addressed or not addressed at all.

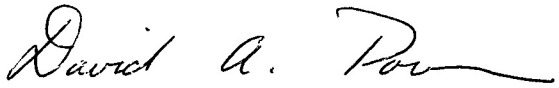
Agency Comments and Our Evaluation

We received written comments on a draft of this report from DHS (see app. II). In the response, the Director, Departmental GAO/OIG Liaison, concurred with our recommendation. The director also proposed replacing the term "cyber assets" with "cyber infrastructure" to broaden the recommendation and update the Assistant Secretary's title. We agreed and addressed his comments accordingly. In addition, the director 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. Furthermore, DHS provided technical comments that have been addressed in this report as appropriate.

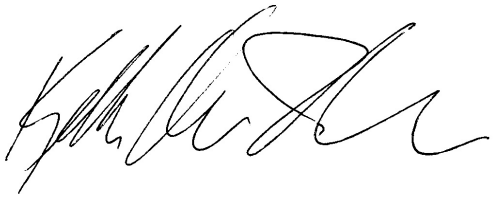
We are sending copies of this report to interested congressional committees, the Secretary of Homeland Security, and other interested parties. We also will make copies available to others upon request. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

Should you or your staffs have any questions on matters discussed in this report, please contact Dave Powner at (202) 512-9286 or pownerd@gao.gov, or Keith Rhodes at (202) 512-6412, or rhodesk@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 key contributions to this report are listed in appendix III.



David A. Powner
Director, Information Technology
Management Issues



Keith A. Rhodes
Chief Technologist
Applied Research and Methods
Center for Technology and Engineering

Appendix I: Briefing for Congressional Staff

Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

Briefing for the

House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

August 7, 2007

and the

Senate Committee on Homeland Security and Governmental Affairs

August 20, 2007

Table of Contents

2

Introduction

Because the nation's critical infrastructure relies extensively on computerized information systems and electronic data, the security of those systems and information is essential to our nation’s security, economy, and public health and safety. To help address critical infrastructure protection, federal policy established a framework for public and private sector partnerships and identified 17 critical infrastructure sectors, including banking and finance, information technology, telecommunications, energy, and public health and healthcare.

The Department of Homeland Security (DHS) is a key player in these partnerships and is responsible for developing a National Infrastructure Protection Plan (NIPP) as a road map for how DHS and other relevant stakeholders are to enhance the protection of critical infrastructure. Lead federal agencies, referred to as sector-specific agencies (including DHS, Treasury, and Health and Human Services), are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

DHS issued NIPP in June 2006. It is a base plan that is to serve as a road map for how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across the sectors in an integrated, coordinated fashion.

3

Introduction

NIPP required each of the lead federal agencies associated with the 17 critical infrastructure sectors to develop plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets 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 programs to protect these assets.

Two DHS organizations that have responsibilities associated with the NIPP and sector-specific plans:

- The Office of Infrastructure Protection (OIP) has responsibility for overseeing and coordinating the development of the plans and tracking and reporting on the progress of implementation. In addition, OIP is responsible for 5 sectors (chemical, commercial facilities, dams, emergency services, and nuclear).
- The Office of Cyber Security and Communication (CS&C) has responsibility for developing, maintaining, and updating the cyber aspects of the NIPP and providing assistance to all sector-specific agencies in developing and implementing the cyber aspects of their respective sector-specific plans. In addition, CS&C is responsible, as the designated sector-specific agency, for the information technology and communications sectors.

4

Objectives, Scope, and Methodology

As requested, our objective was to determine if the sector-specific plans address key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans.

We analyzed DHS's guidance provided to the critical infrastructure sectors that stated how the sectors should address cyber aspects in their sector-specific plans which were to be structured in eight major sections. From this analysis, we identified 30 cyber-related criteria within the 8 sections. DHS officials from CS&C generally agreed with the criteria we developed. Table 1 on the following slide shows the 8 major sections and the 30 associated criteria.

5

GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

Table 1: Cyber-Related Sections

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 (R&D)

- 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 R&D initiatives
- Identifies existing cyber-related projects that support goals and identifies gaps
- Identifies R&D 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

6

Objectives, Scope, and Methodology

We then analyzed the sector-specific plans of the 17 critical infrastructures to determine the extent to which each plan addressed the 30 cyber-related criteria. The following categories were used:

- *fully addressed:* the plan specifically addressed the cyber-related criteria
- *partially addressed:* the plan addressed parts of the criteria or did not clearly address the cyber-related criteria
- *not addressed:* the plan did not specifically address the cyber-related criteria

We met with DHS/CS&C officials to discuss their review and analysis of the plans, as well as our review and analysis of the plans. In addition, DHS/OIP and CS&C officials provided information related to their initiatives to improve the plans. We did not interview officials from the sector-specific agencies or sector representatives or review the adequacy of the sector's actions to address cyber security within their respective sectors.

Our work was performed at DHS/CS&C in Arlington, Virginia, from February 2007 to July 2007 in accordance with generally accepted government auditing standards.

7

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 the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as the agriculture and food and commercial facilities sectors—were not as comprehensive.

In addition to the varying degrees with which the sector-specific plans addressed the 30 section criteria, 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.

Without comprehensive plans, certain sectors may not be adequately identifying, prioritizing, and protecting the cyber aspects of their critical infrastructure protection efforts. Specifically, 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.

8

Results in Brief

The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying level of maturity of the different sectors: that is, sectors whose stakeholders had more experience working together on critical infrastructure issues generally had more comprehensive and complete plans than those with less prior experience.

To assist the sectors in securing their cyber assets, we are recommending that the Secretary of Homeland Security direct the Assistant Secretary for Infrastructure Protection and the Assistant Secretary for Cyber Security and Communication to request that by September 2008 the sector-specific agencies' plans address the cyber-related criteria that were only partially addressed or not addressed.

9

Background

Consistent with the Homeland Security Act of 2002, Homeland Security Presidential Directive-7 (1) established DHS as the principal federal agency to lead, integrate, and coordinate implementation of efforts to protect critical infrastructure and key resources and (2) identified lead federal agencies, referred to as sector-specific agencies, that are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors. It also required DHS to develop a comprehensive and integrated plan by December 2004 that outlines national goals, objectives, milestones, and key initiatives necessary for fulfilling its responsibilities for physical and cyber critical infrastructure protection.

In 2005, we reported on the status of DHS's key cyber security responsibilities, which included developing a NIPP.[1] During this time, DHS had issued an interim NIPP for improving critical infrastructure protection that included cyber security, but that this plan was not yet comprehensive and complete. For example, we reported that the plan did not include sector-specific cyber security plans, lacked required milestones, and was not yet final. We recommended that the Secretary of Homeland Security strengthen the department's ability to implement key cyber security responsibilities.

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

10

Background

In June 2006, DHS issued a final NIPP. This base plan is to serve as a road map for how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion. Further, NIPP required the lead agencies of the 17 critical infrastructure sectors to develop sector-specific plans to address how the sector's stakeholders would implement the national plan and how each sector would improve the security of its assets systems, networks, and functions. The sector-specific plans are to be developed by the designated sector-specific agencies in coordination with relevant government and private-sector representatives.

The plans are important because they are to

- describe how the sector will identify and prioritize its critical assets, including cyber assets such as networks;
- identify the approaches the sector will take to assess risks and develop programs to manage and mitigate risk;
- define the security roles and responsibilities of members of the sector; and
- establish the methods that members will use to interact and share information related to the protection of critical infrastructure.

11

Background

DHS is to use these individual plans to evaluate whether any gaps exist in the protection of critical infrastructures on a national level and, if so, to work with the sectors to address them. The plans are an important step in identifying risk management practices to be implemented, which could improve the security of our nation's cyber-reliant critical infrastructure. These plans do not identify the actual assets and vulnerabilities. Instead, the plans identify the approaches the sector will take to protect their critical cyber infrastructure.

DHS announced the release of the plans for the 17 sectors on May 21, 2007; 7 have been released publicly.[2] The sectors were to provide status updates to DHS by July 1, 2007. DHS plans to incorporate these status reports into an overall critical infrastructure/key resources (CI/KR) report, the "National CI/KR Protection Annual Report," which is due by September 1 of every year to the Executive Office of the President.

[2]New, published versions of the plans are due every 3 years; however, new internal versions of the plans are to be completed every year.

12

Cyber Security Aspects of Sector-Specific Plans

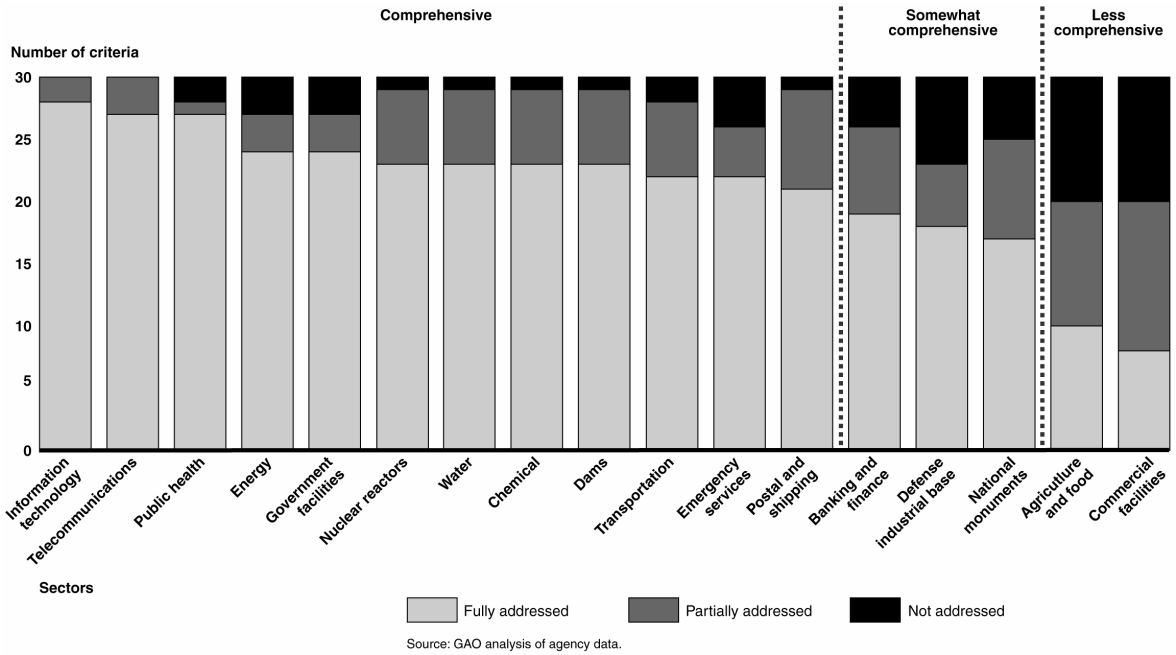
The extent to which the sectors addressed aspects of cyber security in their sector-specific plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several plans—including the information technology and telecommunications sectors—fully addressed many of the criteria and 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.

13

GAO
Accountability * Integrity * Reliability

Cyber Security Aspects of Sector-Specific Plans

Figure 1: Comprehensiveness of Sector-Specific Plans



Source: GAO analysis of agency data.

Attachment 1 contains the detailed results of our analysis showing to what extent each sector plan addressed each criterion.

14

Cyber Security Aspects of Sector-Specific Plans

In addition to the variation in the extent to which the plans covered aspects of cyber security, there was also variance among plans in the extent to which certain criteria were addressed.

All of the plans fully addressed the following criteria:

- identifying a sector governance structure for research and development;
- describing how the sector-specific agency intends to manage its NIPP responsibilities; and
- describing the sector's coordinating mechanisms and structures.

At least 15 of the plans fully addressed the following criteria:

- characterizing the sector's infrastructure, including the cyber reliance;
- identifying stakeholder relationships for securing cyber assets;
- describing a process for updating, reporting, budgeting, and training; and
- describing a process for cyber-related information sharing.

15

Cyber Security Aspects of Sector-Specific Plans

Fewer than half of the plans fully addressed the following criteria:

- describing a process to identify potential consequences of cyber attacks;
- describing any incentives used to encourage voluntary performance of risk assessments;
- developing and using cyber metrics to measure progress; and
- identifying existing cyber-related projects that support goals and identify gaps.

Attachment 2 contains the detailed results of our analysis and shows to what extent the sector-specific plans address each of the 30 criteria.

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

16

Cyber Security Aspects of Sector-Specific Plans

The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying level of maturity of the different sectors. According to DHS officials, the sectors that have been working together longer on critical infrastructure issues generally have more comprehensive and complete plans than the sectors with stakeholders without prior experience working together for a common goal. For example, the plan for the energy sector included most of the key information required for each plan element. This is a result of this sector having a history of working to plan and accomplish many of the same activities that are being required for the sector-specific plans. In addition, according to DHS officials, the chemical sector had worked with DHS to improve the cyber component in its plans; this sector's plan was among those categorized as comprehensive.

Further, for those sectors that had not been working together earlier on critical infrastructure issues and were thus less mature, the limited amount of time to complete the plans was a factor in their plans being less comprehensive and complete. The sectors had 6 months from the time the NIPP was completed—June 2006—and when plans were to be completed—December 2006.

17

Cyber Security Aspects of Sector-Specific Plans

DHS acknowledges the GAO-identified shortcomings in the plans. DHS officials stated that the 17 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 nation's critical infrastructure.

18

Conclusions

The sector-specific plans varied in how comprehensively they addressed the cyber security aspects of their sectors. Without comprehensive plans, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets; be prepared to respond to a significant attack; or identify the cyber risks they face. 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 selected sectors' efforts will remain insufficient to enhance the protection of their computer-reliant assets.

19

Recommendation

To assist the sectors in securing their cyber assets, we are recommending that the Secretary of Homeland Security direct the Assistant Secretary for Infrastructure Protection and the Assistant Secretary for Cyber Security and Communication to request that by September 2008 the sector-specific agencies' plans address the cyber-related criteria that were only partially addressed or not addressed at all.

20

Agency Comments

In commenting on a draft of this briefing, DHS officials generally agreed with our findings and recommendations. They also provided technical comments, which we have incorporated into this briefing, as appropriate.

21

Attachment 1
Summary Analysis of Individual Sector Specific Plans

The following 17 slides summarize our analysis of whether each sector-specific plan *fully*, *partially*, or *did not* address the 30 cyber security-related criteria.

22

Attachment 1
Agriculture and Food

Total amounts: fully addressed = 10; partially addressed = 10; not addressed = 10

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	P
Describes process to identify cyber dependencies/independences	N
Section 3: Assessing Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	P
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	P
Describes methodology for threat analyses of cyber aspects	P
Describes incentives to encourage voluntary vulnerability assessments	P
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	P
Section 5: Developing and Implementing Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	P
Identifies programs to deter, respond, and recover from cyber attack	N
Addresses implementation and maintenance of protective programs	P

Section 6: Measuring Progress	
Ensures that integration of cyber metrics is part of measurement process	N
Describes how cyber metrics will be reported to DHS	N
Includes developing and using cyber metrics to measure progress	N
Describes how to use metrics to guide future cyber projects	N
Section 7: Critical Infrastructure Protection R&D	
Describes how technology developments are related to the sector's cyber	N
Describes process to identify cyber security technology requirements	P
Describes process to solicit information on ongoing cyber R&D initiatives	N
Identifies existing cyber-related projects that support goals and identifies gaps	N
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	N
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

23

Attachment 1
Banking and Finance

Total amounts: fully addressed = 19; partially addressed = 7; not addressed = 4

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	P
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	P
Describes process to identify cyber dependencies/independences	P
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Screening process for cyber aspects	P
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	F
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	N
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	P
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	P
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	N
Identifies existing cyber-related projects that support goals and identifies gaps	N
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	P
Describes sector's coordination structure	F
Describes process for investment priorities	N
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

24

Attachment 1
Chemical

Total amounts: fully addressed = 23; partially addressed = 6; not addressed = 1

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	P
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	P
Describes how cyber metrics will be reported to DHS	P
Includes developing and using cyber metrics to measure progress	P
Describes how to use metrics to guide future cyber projects	P
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

25

Attachment 1
Commercial Facilities

Total amounts: fully addressed = 8; partially addressed = 12; not addressed = 10

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	P
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	N
Describes process to identify cyber dependencies/independences	N
Section 3: Assess Risks	
How risk assessment process addresses cyber elements	P
Describes a screening process for cyber aspects	P
Describes methodology to identify potential consequences of cyber attacks	N
Describes methodology for vulnerability assessments of cyber aspects	N
Describes methodology for threat analyses of cyber aspects	N
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	P
Describes criteria and basis for prioritization of cyber aspects	P
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	N
Describes process to identify specific cyber-related program needs	P
Identifies programs to deter, respond, and recover from cyber attack	P
Addresses implementation and maintenance of protective programs	P

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	N
Describes how cyber metrics will be reported to DHS	P
Includes developing and using cyber metrics to measure progress	N
Describes how to use metrics to guide future cyber projects	N
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	P
Describes process to identify cyber security technology requirements	P
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	P
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

26

Attachment 1
Dams

Total amounts: fully addressed = 23; partially addressed = 6; not addressed = 1

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	P
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	P
Describes incentives to encourage voluntary vulnerability assessments	P
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	P
Includes developing and using cyber metrics to measure progress	N
Describes how to use metrics to guide future cyber projects	P
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals & identifies gaps	P
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

27

Attachment 1
Defense Industrial Base

Total amounts: fully addressed = 18; partially addressed = 5; not addressed = 7

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	P
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
How risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	N
Describes methodology to identify potential consequences of cyber attacks	N
Describes methodology for vulnerability assessments of cyber aspects	N
Describes methodology for threat analyses of cyber aspects	N
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	P
Describes criteria and basis for prioritization of cyber aspects	N
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	P
Describes process to identify specific cyber-related program needs	P
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	N
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	P

Key: F = fully addressed P = partially addressed N = not addressed

28

GAO
Accountability * Integrity * Reliability

Attachment 1
Emergency Services

Total amounts: fully addressed = 22; partially addressed = 4; not addressed = 4

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	P
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	P
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	N
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	N
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	P
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	N
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

29

Attachment 1
Energy

Total amounts: fully addressed = 24; partially addressed = 3; not addressed = 3

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
How risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	N
Describes criteria and basis for prioritization of cyber aspects	N
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	P
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	P
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	P
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

30

Attachment 1
Government Facilities

Total amounts: fully addressed = 24; partially addressed = 3; not addressed = 3

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	P
Identifies stakeholder relationships for securing cyber assets	P
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	N
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	N
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	P
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

31

GAO
Accountability * Integrity * Reliability

Attachment 1
Information Technology

Total amounts: fully addressed = 28; partially addressed = 2; not addressed = 0

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	P
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	P
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

32

Attachment 1

National Monuments and Icons

Total amounts: fully addressed = 17; partially addressed = 8; not addressed = 5

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	N
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	P
Describes incentives to encourage voluntary vulnerability assessments	P
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	P
Describes criteria and basis for prioritization of cyber aspects	P
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	N
Describes how cyber metrics will be reported to DHS	N
Includes developing and using cyber metrics to measure progress	N
Describes how to use metrics to guide future cyber projects	N
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	P
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	P
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	P
Describes process for cyber-related information sharing	P

Key: F = fully addressed P = partially addressed N = not addressed

33

Attachment 1
Nuclear Reactors, Waste, Materials

Total amounts: fully addressed = 23; partially addressed = 6; not addressed = 1

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	P
Identifies programs to deter, respond, and recover from cyber attack	P
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	P
Describes how cyber metrics will be reported to DHS	P
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	P
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

34

Attachment 1
Postal and Shipping

Total amounts: fully addressed = 21; partially addressed = 8; not addressed = 1

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	P
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	F
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	P
Addresses implementation and maintenance of protective programs	P

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	N
Describes how cyber metrics will be reported to DHS	P
Includes developing and using cyber metrics to measure progress	P
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	P
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	P
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

35

Attachment 1
Public Health and Healthcare

Total amounts: fully addressed = 27; partially addressed = 1; not addressed = 2

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	N
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	N
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

36

Attachment 1
Telecommunications

Total amounts: fully addressed = 27; partially addressed = 3; not addressed = 0

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	P
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	P
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	F
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

37

Attachment 1
Transportation

Total amounts: fully addressed = 22; partially addressed = 6; not addressed = 2

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	P
Describes a screening process for cyber aspects	N
Describes methodology to identify potential consequences of cyber attacks	P
Describes methodology for vulnerability assessments of cyber aspects	F
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	P
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	F
Describes process to identify specific cyber-related program needs	F
Identifies programs to deter, respond, and recover from cyber attack	F
Addresses implementation and maintenance of protective programs	P

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	F
Describes how to use metrics to guide future cyber projects	F
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	P
Describes process to solicit information on ongoing cyber R&D initiatives	P
Identifies existing cyber-related projects that support goals and identifies gaps	N
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

38

GAO
Accountability * Integrity * Reliability

Attachment 1
Water

Total amounts: fully addressed = 23; partially addressed = 6; not addressed = 1

Section 1: Sector Profile and Goals	
Characterizes cyber aspects	F
Identifies stakeholder relationships for securing cyber assets	F
Section 2: Identify Assets, Systems, Networks, and Functions	
Describes process to identify cyber assets, functions, or elements	F
Describes process to identify cyber dependencies/independences	F
Section 3: Assess Risks	
Describes how the risk assessment process addresses cyber elements	F
Describes a screening process for cyber aspects	F
Describes methodology to identify potential consequences of cyber attacks	F
Describes methodology for vulnerability assessments of cyber aspects	P
Describes methodology for threat analyses of cyber aspects	F
Describes incentives to encourage voluntary vulnerability assessments	F
Section 4: Prioritizing Infrastructure	
Identifies entity responsible for prioritization of cyber aspects	F
Describes criteria and basis for prioritization of cyber aspects	F
Section 5: Develop and Implement Protective Programs	
Describes process to develop long-term protective-plans for cyber aspects	P
Describes process to identify specific cyber-related program needs	P
Identifies programs to deter, respond, and recover from cyber attack	N
Addresses implementation and maintenance of protective programs	F

Section 6: Measure Progress	
Ensures that integration of cyber metrics is part of measurement process	F
Describes how cyber metrics will be reported to DHS	F
Includes developing and using cyber metrics to measure progress	P
Describes how to use metrics to guide future cyber projects	P
Section 7: CI/KR Protection R&D	
Describes how technology developments are related to the sector's cyber	F
Describes process to identify cyber security technology requirements	P
Describes process to solicit information on ongoing cyber R&D initiatives	F
Identifies existing cyber-related projects that support goals and identifies gaps	F
Identifies R&D governance structure	F
Section 8: Managing and Coordinating SSA responsibilities	
Describes sector-specific agency's management of NIPP responsibilities	F
Describes process for updating, reporting, budgeting, and training	F
Describes sector's coordination structure	F
Describes process for investment priorities	F
Describes process for cyber-related information sharing	F

Key: F = fully addressed P = partially addressed N = not addressed

39

GAO
Accountability * Integrity * Reliability

Attachment 2
Overall Summary Analysis of Sector Specific Plans

The following table illustrates the number of plans that *fully*, *partially*, and did *not address* each criterion.

Criteria	No. of plans that fully addressed	No. of plans that partially addressed	No. of plans that did not address
Section 1: Sector Profile and Goals			
Characterizes the sector infrastructure, including cyber reliance	15	2	0
Identifies stakeholder relationships for securing cyber assets	15	2	0
Section 2: Identify Assets, Systems, Networks, and Functions			
Describes process to identify cyber assets, functions, or elements	13	3	1
Describes process to identify cyber dependencies/independences	13	1	3
Section 3: Assessing Risks			
Describes how the risk assessment process addresses cyber elements	14	3	0
Describes a screening process for cyber aspects	9	5	3
Describes methodology to identify potential consequences of cyber attacks	7	8	2
Describes methodology for vulnerability assessments of cyber aspects	13	2	2
Describes methodology for threat analyses of cyber aspects	11	4	2
Describes incentives to encourage voluntary vulnerability assessments	3	6	8
Section 4: Prioritizing Infrastructure			
Identifies entity responsible for prioritization of cyber aspects	11	4	2
Describes criteria and basis for prioritization of cyber aspects	12	3	2

40

GAO
Accountability * Integrity * Reliability

Attachment 2

Overall Summary Analysis of Sector Specific Plans

Criteria	No. of plans that fully addressed	No. of plans that partially addressed	No. of plans that did not address
Section 5: Developing and Implementing Protective Programs			
Describes process to develop long-term protective-plans for cyber aspects	13	3	1
Describes process to identify specific cyber-related program needs	11	6	0
Identifies programs to deter, respond, and recover from cyber attack	9	3	5
Addresses implementation and maintenance of protective programs	13	4	0
Section 6: Measuring Progress			
Ensures that integration of cyber metrics is part of measurement process	9	3	5
Describes how cyber metrics will be reported to DHS	9	6	2
Includes developing and using cyber metrics to measure progress	8	5	4
Describes how to use metrics to guide future cyber projects	10	4	3
Section 7: Critical Infrastructure Protection R&D			
Describes how technology developments are related to the sector's cyber goals	14	2	1
Describes process to identify cyber security technology requirements	11	6	0
Describes process to solicit information on ongoing cyber R&D initiatives	13	2	2
Identifies existing cyber-related projects that support goals & identifies gaps	7	5	5
Identifies R&D governance structure	17	0	0
Section 8: Managing and Coordinating SSA responsibilities			
Describes sector-specific agency's management of NIPP responsibilities	17	0	0
Describes process for updating, reporting, budgeting, and training	16	1	0
Describes sector's coordination structure	17	0	0
Describes process for investment priorities	14	1	2
Describes process for cyber-related information sharing	15	2	0

41

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

October 16, 2007

Mr. David A. Powner
Director, Information Technology
Management Issues
Government Accountability Office
Washington, DC20548

Dear Mr. Powner:

Re: Draft Report GAO-07-1191, Critical Infrastructure Protection Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies.

Thank you for the opportunity to review the draft report.

The following represents the Department's response to the GAO recommendation.

Recommendation:

To assist the sectors in securing their cyber assets, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for Infrastructure Protection and the Assistant Secretary for Cyber Security and Communication to request that by September 2008 the sector-specific agencies' plans address the cyber related criteria that were only partially addressed or not addressed at all.

Response:

Concur. However, we propose a revision to the recommendation as follows To assist the sectors in securing their cyber infrastructure, we are recommending 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 only partially addressed or not addressed.

Rationale: Infrastructure is a broader term than assets. Suggest using infrastructure for consistency with NIPP concept of assets, systems, networks, and functions.

www.dhs.gov

DHS has adopted the language of Section 514 of the Homeland Security Act (6 U.S.C. 321c(b)) establishing the position of Assistant Secretary for **"Cybersecurity"** and Communications.

The Cybersecurity and Communications National Cyber Security Division is currently working on an action plan to assist sectors in addressing cyber security issues not adequately addressed in the initial Sector-Specific Plans (SSPs).

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

David A. Powner at (202) 512-9286 or pownerd@gao.gov
Keith A. Rhodes at (202) 512-6412 or rhodesk@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following also made key contributions to this report: Scott Borre, Barbara Collier, Neil Doherty, Michael Gilmore, Nancy Glover, Franklin Jackson, Barbarol James, and Eric Winter.

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

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548