

September 2009

CRITICAL INFRASTRUCTURE PROTECTION

Current Cyber Sector-Specific Planning Approach Needs Reassessment



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-09-969](#), a report to congressional requesters

Why GAO Did This Study

The nation's critical infrastructure sectors (e.g., energy, banking) rely extensively on information technology systems. The Department of Homeland Security (DHS) issued guidance in 2006 that instructed lead federal agencies, referred to as sector-specific agencies, to develop plans for protecting the sector's critical cyber and other (physical) infrastructure. These agencies issued plans in 2007, but GAO found that none fully addressed all 30 cyber security-related criteria identified in DHS's guidance and recommended that the plans be updated to address it by September 2008. GAO was asked to determine the extent to which sector plans have been updated to fully address DHS's cyber security requirements and assess whether these plans and related reports provide for effective implementation. To do this, GAO analyzed documentation, interviewed officials, and compared sector plans and reports with DHS cyber criteria.

What GAO Recommends

GAO recommends that DHS assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure and consider whether other options would provide more effective results. DHS concurred with the recommendation; however, it took exception with certain report facts and conclusions. GAO addressed these comments, but they did not result in substantive report revisions.

View [GAO-09-969](#) or [key components](#). For more information, contact David Powner, 202-512-9286, pownerd@gao.gov.

CRITICAL INFRASTRUCTURE PROTECTION

Current Cyber Sector-Specific Planning Approach Needs Reassessment

What GAO Found

Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies have yet to update their respective sector-specific plans to fully address key DHS cyber security criteria. For example, of the 17 sector-specific plans, only 9 have been updated. Of these 9 updates, just 3 addressed missing cyber criteria, and those 3 involved only a relatively small number (3 or fewer) of the criteria in question. Recently DHS issued guidance specifically requesting that the sectors address cyber criteria shortfalls in their 2010 sector-specific plan updates. Until the plans are issued, it is not clear whether they will fully address cyber requirements. Accordingly, the continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach and thus increases the risk that the nation's cyber assets have not been adequately identified, prioritized, and protected.

Most sector-specific agencies developed and identified in their 2007 sector plans those actions—referred to by DHS as implementation actions—essential to carrying out the plans; however, since then, most agencies have not updated the actions and reported progress in implementing them as called for by DHS guidance. Specifically, in response to 2006 guidance that called for agencies to address three key implementation elements (action descriptions, completion milestones, and parties responsible), most sectors initially developed implementation actions that fully addressed the key elements. However, while 2008 guidance called for implementation actions to be updated and for sector reports to include progress reporting against implementation action milestone commitments, only five sectors updated their plans and reported on progress against implementation actions. DHS attributed this in part to the department not following up and working to ensure that all sector plans are fully developed and implemented in accordance with department guidance.

The lack of complete updates and progress reports are further evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where it stands in securing cyber critical infrastructures. Not following up to address these conditions also shows DHS is not making sector planning a priority. Further, recent studies by a presidential working group—which resulted in the President establishing the White House Office of Cybersecurity Coordinator—and an expert commission also identified shortfalls in the effectiveness of the current public-private partnership approach and related sector planning and offered options for improving the process. Such options include (1) prioritizing sectors to focus planning efforts on those with the most important cyber assets and (2) streamlining existing sectors to optimize their capacity to identify priorities and develop plans. Given this, it is essential that DHS and the to-be-appointed Cybersecurity Coordinator determine whether the current process as implemented should continue to be the national approach and thus worthy of further investment.

Contents

Letter		1
	Sector-Specific Agencies Have Yet to Update Their Respective Sector-Specific Plans to Fully Address Key Cyber Security Criteria as Called for by DHS Guidance	3
	Sector Plans and Related Reports Do Not Fully Provide For Effective Implementation	3
	Conclusions	4
	Recommendations	4
	Agency Comments and Our Evaluation	5
Appendix I	Briefing Provided to Staff, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, House Committee on Homeland Security	11
Appendix II	Comments from the Department of Homeland Security	55
Appendix III	GAO Contact and Staff Acknowledgments	61

Abbreviations

CIP	critical infrastructure protection
DHS	Department of Homeland Security
IT	information technology
NIPP	National Infrastructure Protection Plan
SSP	sector-specific plan

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.



United States Government Accountability Office
Washington, DC 20548

September 24, 2009

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

The Honorable James R. Langevin
House of Representatives

The nation's critical infrastructure relies extensively on computerized information technology (IT) systems and electronic data. The security of those systems and information is essential to the nation's security, economy, and public health and safety. To help protect critical infrastructure, federal policy established a framework for public and private sector partnerships and identified 18 critical infrastructure sectors such as energy and banking and finance. To implement the framework, the Department of Homeland Security (DHS) issued a 2006 National Infrastructure Protection Plan that along with other DHS guidance, called for lead federal agencies (sector-specific agencies) to develop sector-specific plans and sector annual reports to address how sectors would implement the national plan, including how key cyber infrastructure assets were to be protected—commonly referred to as cyber security. In May 2007, sector-specific agencies issued plans for their sectors; we subsequently reviewed the plans and reported¹ that none fully addressed 30 cyber security-related criteria identified in DHS's guidance and recommended that DHS request that the sector-specific agencies' plans address the cyber-related criteria by September 2008.

Since then, an expert commission—led by two congressmen and industry officials—studied and reported in late 2008 on the public-private partnership, including sector planning approach and other aspects of U.S. cyber security policy. More recently, the President established (1) a cyber security working group that completed a “60-day” review of federal cyber policy and (2) a Cybersecurity Coordinator (the position has not yet been

¹GAO, *Critical Infrastructure Protection: Sector-Specific Plans/ Coverage of Key Cyber Security Elements Varies*. [GAO-08-113](#) (Washington, D.C.: Oct. 31, 2007).

filled) within the White House to assist in developing new cyber policies and coordinating efforts across the federal government. Both studies identified issues with the current sector planning as well as options to improve it.

This report responds to your request that we (1) determine the extent to which sector plans have been updated to fully address DHS cyber security requirements and (2) assess whether these plans and related reports provide for effective implementation.

On July 29, 2009, we provided a briefing to staff of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, House Committee on Homeland Security. This report summarizes and transmits (1) the presentation slides we used to brief the staff and (2) recommendations to the Secretary of Homeland Security that are part of those slides. The full briefing, including our scope and methodology, is reprinted as appendix I. We conducted this performance audit from October 2008 to September 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Sector-Specific Agencies Have Yet to Update Their Respective Sector-Specific Plans to Fully Address Key Cyber Security Criteria as Called for by DHS Guidance

Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies have yet to update their respective sector-specific plans to fully address key DHS cyber security criteria. For example, of the 17² sector-specific plans, only 9 have been updated. Of these 9 updates, just 3 addressed missing cyber criteria, and those 3 involved only a relatively small number (3 or fewer) of the criteria in question. Sector-specific agencies did not fully address missing cyber criteria in their plans in large part due to the following:

- They were focused more on the physical rather than the cyber security aspects of the criteria in preparing their plans.
- They were unaware of the cyber criteria shortfalls identified in 2007.
- DHS's guidance on updating sector plans did not specifically request the agencies to update the cyber security aspects of their plans.

The continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach and thus increases the risk that the nation's cyber assets have not been adequately identified, prioritized, and protected.

Sector Plans and Related Reports Do Not Fully Provide For Effective Implementation

Most sector-specific agencies developed and identified in their 2007 sector plans those actions—referred to by DHS as implementation actions—essential to carrying out the plans; however, since then, most agencies have not updated the actions and reported progress in implementing them as called for by DHS guidance. Specifically, in response to 2006 guidance that called for agencies in developing implementation actions to address three key elements (action descriptions, completion milestones, and responsible parties), most sectors initially developed implementation actions that fully addressed the key elements. However, while 2008 guidance called for implementation actions to be updated and for sector reports to include progress reporting against implementation action milestone commitments, only five sectors updated their plans and reported on implementation progress. DHS attributed this in part to the department not following up and working to ensure that all sector plans

²Currently, there are 18 sectors; however, one sector (critical manufacturing) was established in 2008 and has not yet completed a sector-specific plan.

are fully developed and implemented in accordance with department guidance. The lack of complete updates and progress reports are further evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where we stand in securing cyber-critical infrastructures.

Conclusions

Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies have made limited progress in updating their sector-specific plans to fully address key cyber elements. Further, although the agencies produced narratives on sector activities, they have not developed effective implementation actions and reported on whether progress is being made in implementing their sector plans. This means that as a nation, we do not know precisely where we are in implementing sector plans and associated protective measures designed to secure and protect the nation's cyber and other critical infrastructure, despite having invested many years in this effort. This condition is due in part to DHS not making sector planning a priority and as such, not managing it in a way that fully meets DHS guidance. These conclusions, taken as a whole, further raise fundamental questions about whether the current approach to sector planning is worthwhile and whether there are options that would provide better results. Consequently, it is essential that federal cyber security leaders—including DHS and the to-be-appointed Cybersecurity Coordinator—exert their leadership roles in this area by, among other things, determining whether it is worthwhile to continue with the current approach as implemented or consider if proposed options provide more effective results. To do less means the nation's critical infrastructure sectors will continue to be at risk of not being able to adequately protect their cyber and other critical assets or be prepared to identify and respond to cyber threats and vulnerabilities.

Recommendations

We recommend that the Secretary of Homeland Security, consistent with any direction from the Office of the Cybersecurity Coordinator, assess whether the existing sector-specific planning process should continue to be the nation's approach to securing cyber and other critical infrastructure and, in doing so, consider whether proposed and other options would provide more effective results.

If the existing approach is deemed to be the national approach, we also recommend that the Secretary make it, including the cyber aspects, an

agency priority and manage it accordingly. This should include collaborating closely with other sector-specific agencies to develop

- sector-specific plans that fully address cyber-related criteria in the next release of the plans, and
- sector annual reports that (1) include updated implementation actions and associated milestones and (2) report progress against plan commitments and timelines.

Agency Comments and Our Evaluation

DHS concurred with our recommendations but took exception with certain report facts and conclusions that it said formed the basis for our recommendations. Specifically, in an email accompanying its written response—which was signed by the Director, Departmental GAO/OIG Liaison Office and is reprinted in appendix II—DHS said it concurred with our recommendation. In its written response, DHS added that it supported continually assessing the effectiveness of the sector approach and identifying and implementing improvements as appropriate. The department also stated in its written response that alternative options can be explored and implemented along with the current sector approach, rather than a binary choice between continuing the existing sector-specific planning approach and other options. We agree such efforts can be pursued in parallel and that doing them in this manner would be consistent with our recommendations. The department also commented that the report does not give due consideration to many of the ongoing sector and cross-sector cyber security activities identified in the annual reports and briefed to us. We recognize that DHS has multiple ongoing efforts to improve critical infrastructure protection (CIP) planning and implementation, and our report conclusions state this point. While our report for the sake of brevity does not include all of DHS's efforts, it does include illustrative examples throughout as part of giving a fair and balanced view of DHS's efforts in this area.

Notwithstanding the concurrence discussed above, DHS in its written response took exception with our report's facts and conclusions in nine areas—referred to by DHS as general items. Each of these general items, along with our response, is summarized below.

General item 1: With regard to our report section that states that the sector-specific agencies have yet to update their respective plans to fully address key cyber security criteria as called for by DHS, the department commented that it established a risk management framework (as part of

the 2006 National Infrastructure Protection Plan or NIPP) which called for cyber and other elements (i.e., human, physical) to be addressed. DHS added that its 2006 SSP guidance did not call for these elements to be addressed separately in the plans and at that time GAO had not identified the 30 cyber criteria in DHS's guidance; therefore, when the 2007 SSPs were issued they did not fully address the 30 cyber criteria (which is consistent with our October 2007 report findings). To address this situation, DHS said it revised the NIPP in early 2009 to, among other things, provide for more robust coverage of cyber security using as a basis the 30 cyber criteria identified by GAO. In addition, in its guidance to the sector agencies in developing their 2010 SSPs, DHS directed the agencies to update their plans using the revised NIPP and in doing so, to fully address the 30 GAO-identified cyber criteria.

GAO response: It is a positive development that DHS has issued guidance directing the sector agencies to fully address missing cyber criteria as part of having the sectors rewrite their SSPs in 2010.

In addition, while we agree with DHS that its 2006 guidance did not call for cyber to be addressed separately in each SSP section, it is important to point out that DHS's 2006 guidance nonetheless called for the sectors to address in the SSPs how they planned to secure the cyber aspects of their critical infrastructures. Consequently, the 2007 SSPs were to have addressed cyber in order to be in compliance with DHS's guidance.

In 2007, we initiated a review to assess the extent to which these plans addressed cyber. As part of that review, we analyzed the 2006 guidance and identified 30 cyber-related criteria that the critical infrastructure sectors were to address in their SSPs. Our analysis of the plans found them to be lacking in the cyber area and we subsequently recommended³ that DHS request that by September 2008, the sector agencies update their SSPs to address missing cyber-related criteria. DHS agreed with this recommendation, and stated that the department had initiated efforts to implement it. However, in following up on this recommendation and analyzing the cyber content of the sectors' 2008 SSP updates (which was the first objective of this report), only 3 of the 17 sectors had updated their plans to address missing criteria.

³[GAO-08-113](#).

General item 2: Regarding the section of our report stating that the reason sector-specific agencies did not fully address missing cyber criteria in their plans was due in part to the fact that they were unaware of the cyber criteria shortfalls identified in our 2007 report, DHS described several initiatives it had taken to inform the agencies of their planning shortfalls.

GAO response: We recognize that DHS has taken actions to inform the agencies of the shortfalls identified in our 2007 report. Accordingly, we cited illustrative examples of such actions throughout our report. Nonetheless, when we interviewed sector agencies officials, several stated that they were unaware of the GAO identified shortfalls, which raises questions about the effectiveness of DHS's efforts.

General item 3: DHS stated that while the SSPs have not been fully updated to include ongoing and planned cyber security activities, it does not mean there is a lack of cyber security planning in the sectors or that the planning to date has been ineffective. DHS also reiterated its earlier point that our report does not take into account many of its ongoing activities in the sector related to cyber security. In addition, the department commented that all the sectors reported on their progress in the 2008 annual reports.

GAO response: We recognize that DHS has had many ongoing efforts related to improving the cyber content of SSPs and illustrative examples are provided throughout our report. However, the sector-specific agencies' limited progress in addressing missing cyber content in their SSPs indicates a lack of effectiveness of planning. Specifically, of the 17 sector-specific plans, only 9 have been updated. Of these 9 updates, just 3 addressed missing cyber criteria, and those 3 only involved a relatively small number (3 or less) of the criteria in question. In our view, this continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach and thus increased the risk that the nation's cyber assets have not been adequately identified, prioritized, and protected.

Further, while we agree with DHS that the sectors reported aspects of progress in the 2008 annual reports, only five sectors updated and reported on the extent of progress in carrying out their implementation actions as called for by DHS guidance, while the other 12 did not. This level of reporting is not sufficient for evaluating sector-wide progress and raises concerns about the effectiveness of these annual reports as a tool to measure progress.

General item 4: DHS commented that (1) we expanded the scope of this engagement beyond the initial focus on coverage of cyber security in the SSPs to encompass the entire sector planning approach and that DHS was not asked to provide a broader update on the public-private partnership, and (2) our draft report did not include information on DHS's numerous ongoing activities with the agencies and sectors related to cyber security.

GAO response: With regard to the first comment, the focus of our engagement was on the cyber security aspects of the sector-specific plans and progress reporting, which are an important part of the sector planning approach. Consequently, even when taking into consideration DHS's ongoing activities with the agencies and sectors related to cyber security, the planning and reporting shortfalls we identified indicate a lack of effectiveness with the current sector approach.

Regarding DHS's second comment, we recognize that DHS has multiple ongoing efforts to improve CIP planning and implementation, and our report includes illustrative examples of DHS's efforts to do so. As a case in point, on July 27, 2009, we briefed DHS using the presentation slides in this report and updated the slides to incorporate examples (in addition to the ones we had already included in the briefing) that DHS described to us during that meeting. Although DHS has many ongoing efforts related to improving the cyber content of SSPs, our analysis showed that there had been limited progress in addressing missing cyber content in the SSPs since our 2007 recommendation; this indicates to us that the planning process lacks effectiveness, which is why we recommended that DHS assess whether improvements are needed to the current process.

General item 5: In regard to our report stating that DHS guidance calls for the sector agencies to annually review and update as appropriate their sector plans, which serve as a means to provide an interim snapshot of where agencies stand in addressing their gaps and is why we used it as a basis to assess progress, DHS said the SSPs are intended to be strategic, three-year plans and are not meant to provide a snapshot of where agencies stand in addressing their gaps and should not be used as a basis to assess progress in CIP protection.

GAO response: Our report acknowledges that the SSPs are high-level strategic plans and the sector annual reports serve as the primary means of assessing progress in improving CIP protection. Specifically, as stated in our report, the annual reports are used to, among other things, capture changes in sector programs and assess progress made against goals set in the SSPs. However, it should be noted that annual updates to the SSPs also

include information on progress being made against SSP goals and as such serve as a source of evidence on where agencies stand in addressing their gaps and provide a basis to assess progress in CIP protection. Specifically, the 2008 updates we reviewed and analyzed included key information on what sector agencies had (or had not) done to address missing cyber security content that we identified in their 2007 SSPs.

General item 6: In response to our reporting that most agencies had not updated their implementation actions and reported progress in implementing them as called for by DHS guidance, DHS commented that many of the implementation actions were one-time actions that were completed in 2007 or 2008, and that others are of an ongoing, continuous nature. The department added that since the vast majority of these items were completed, DHS made adjustments in 2009 to the reporting process to more accurately capture the progress of CIP efforts, and that DHS is now working with the sectors toward the development of outcome-based metrics designed to measure the beneficial value of activities in mitigating CIP risks.

GAO response: We recognize that many of the implementation actions were one-time or ongoing actions, but DHS's guidance nonetheless called for the sectors to update the actions and report on the extent of progress in achieving the actions. Further, we agree that DHS has made recent positive changes to their reporting processes to more accurately capture progress. However, as noted in our report, most sectors had not reported in their 2008 sector annual reports that their implementation actions were completed, which showed that the existing progress reporting process was not totally effective.

General item 7: In response to our reporting that DHS's lack of follow up to address SSP planning shortfalls showed it was not making sector planning a priority, the department stated that it (1) is actively engaged with the agencies and sectors, (2) assists the sectors with planning and reporting on an ongoing basis, and (3) continually evaluates and improves these processes with input from the sectors.

GAO response: We recognize that DHS has multiple ongoing efforts to improve CIP planning and implementation, and our report includes illustrative examples of DHS's efforts. Despite these efforts, DHS's limited progress in addressing missing cyber content in the SSPs since our 2007 recommendation and the lack of updated implementation actions and progress reporting—coupled with the department's limited follow up to correct these conditions—led us to conclude that DHS is not making sector planning a priority.

General item 8: DHS stated that although our report cited the work and studies of an expert commission and the President's cybersecurity working group, including the issues they raised with the current sector planning approach, we did not discuss the reports with the department.

GAO response: On July 27, 2009, we briefed DHS on our findings, conclusions, and recommendations, which included descriptions of the work performed by these two groups. Specifically, in advance of our meeting, we provided the department with a draft of our briefing presentation slides for review and then met to discuss each slide of our presentation, including those addressing the work of these two expert groups.

General item 9: In citing our recommendation that calls for DHS to collaborate closely with the sector-specific agencies to develop SSPs that fully address cyber-related criteria, the department stated this collaboration has already begun as part of the department's current effort to have the sector agencies update their SSPs for issuance in 2010.

GAO response: This effort to collaborate with the agencies is consistent with our recommendations.

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

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



David A. Powner
Director, Information Technology
Management Issues

Appendix I: Briefing Provided to Staff, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, House Committee on Homeland Security



Critical Infrastructure Protection: Current Cyber Sector- Specific Planning Approach Needs Reassessment

Briefing to the Staff of the

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

House Committee on Homeland Security

July 29, 2009



Outline of Briefing

Introduction

Objectives, Scope, and Methodology

Results in Brief

Background

Results

 Objective 1

 Objective 2

Conclusions

Recommendations for Executive Action

Agency Comments and Our Evaluation

Attachment I



Introduction

The nation's critical infrastructure relies extensively on computerized information technology (IT) systems and electronic data. The security of those systems and information is essential to the 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 18 critical infrastructure sectors (e.g., Banking and Finance; Information Technology; Telecommunications; Energy; Agriculture and Food; and Commercial Facilities).

The Department of Homeland Security (DHS) is a key player in these partnerships and is responsible for issuing guidance to direct the sectors to develop plans addressing how key IT systems and data are to be secured, commonly referred to as cyber security.

In June 2006, DHS issued the National Infrastructure Protection Plan (NIPP) as a road map for how DHS and other relevant stakeholders are to enhance the protection of critical infrastructure and how they should 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—are responsible for coordinating critical infrastructure protection efforts with public and private stakeholders within each sector. For example, the Department of Treasury is responsible for the banking and finance sector while the Department of Energy is responsible for the energy sector.



Introduction

Further, the NIPP called for the lead federal agencies to develop sector-specific plans and sector annual reports to address how the sectors would implement the national plan, including how the security of cyber and other (physical) assets and functions was to be improved. More specifically, it stated that the

- sector plans were to, among other things, describe how the sector will identify and prioritize its critical cyber and other assets and define approaches to be taken to assess risks and develop programs to protect these assets; and
- sector annual reports were to provide status and progress on each sector's efforts to carry out the sector plans.



Introduction

In response, the sector-specific agencies developed and issued plans for their sectors in May 2007. Subsequently, in examining these initial plans to determine the extent to which they addressed cyber security, we

- reported¹ in October 2007, that none of the plans fully addressed all 30 cyber security-related criteria we identified in DHS guidance (in performing that work, we (1) analyzed DHS guidance provided to the critical infrastructure sectors that stated how the sectors should address cyber topics in their sector-specific plans, (2) identified 30 cyber-related criteria, and (3) shared them with responsible DHS officials who largely agreed that these were the correct criteria to use), and
- recommended that DHS 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.

¹ GAO, *Critical Infrastructure Protection: Sector-Specific Plans/ Coverage of Key Cyber Security Elements Varies*, [GAO-08-113](#) (Washington, D.C.: Oct. 31, 2007).



Introduction

Since then, an expert commission—led by two congressmen and industry officials—studied and reported² in late 2008 on the public-private partnership approach, including sector planning and other aspects of U.S. cyber security policy.

More recently, the President established a White House cyber security working group that

- conducted and completed a “60-day” review of U.S. cyber policy, including public-private partnerships and sector planning, that found that while sector and other groups involved in the partnership performed valuable work, there were alternative approaches for how the federal government could work with the private sector and recommended that these options be explored, and
- recommended, among other things, establishing a Cybersecurity Coordinator’s position within the White House to develop a new U.S. cyber policy and to coordinate cyber security efforts across the federal government.

² Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C., December 2008); and The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., May 29, 2009).



Objectives, Scope, and Methodology

As agreed, our objectives were to

- determine the extent to which sector plans have been updated to fully address cyber security requirements, and
- assess whether these plans and related reports provide for effective implementation.

For the first objective, we met with the sector-specific agencies to obtain updates to the May 2007 initial plans issued for the 17³ critical infrastructure sectors. We then analyzed any updated plans using the 30 cyber criteria we identified in DHS guidance on how such plans were to be developed. Attachment I shows the 30 criteria (organized by eight major reporting sections called for in the DHS guidance). In particular, we focused on assessing the cyber criteria not fully addressed in the May 2007 plans.

³ Currently, there are 18 sectors; however, the critical manufacturing sector was established in 2008 and has not yet completed a sector-specific plan.



Objectives, Scope, and Methodology

In analyzing the updated plans against the 30 criteria, we categorized the extent to which the plans addressed criteria using the following:

- *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

Further, we also interviewed responsible sector-specific agency officials to, among other things, verify our understanding of their updated sector plans and to validate the accuracy of our analyses of the extent to which additional cyber-related criteria had been addressed in them.



Objectives, Scope, and Methodology

For the second objective, we

- identified requirements in DHS guidance that specified how the sectors were to update and report on their progress in carrying out planned actions—referred to by the department as implementation actions, and
- compared these requirements to what the sectors had reported in their 2008 annual reports.⁴

We focused on the implementation actions, because they are important for reporting and assessing the progress and effectiveness of the sector-specific plans. Where gaps existed, we collaborated with the sector officials to obtain any additional information that would fulfill the requirements and to determine the cause and impact of any remaining gaps.

⁴ The critical manufacturing sector did not have any annual reports.



Objectives, Scope, and Methodology

We conducted this performance audit from October 2008 to July 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



Results in Brief

Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies have yet to update their respective sector-specific plans to fully address key DHS cyber security criteria. For example, of the 17 sector-specific plans, only 9 have been updated. Of these 9 updates, just 3 addressed missing cyber criteria, and those 3 involved only a relatively small number (3 or fewer) of the criteria in question. Sector-specific agencies did not fully address missing cyber criteria in their plans in large part due to the following:

- They were focused more on the physical rather than the cyber security aspects of the criteria in preparing their plans.
- They were unaware of the cyber criteria shortfalls identified in 2007, and
- DHS's guidance on updating sector plans did not specifically request the agencies to update the cyber security aspects of their plans.

Recently DHS issued guidance specifically requesting that the sectors address cyber criteria shortfalls in their 2010 sector-specific plan updates. However, until the plans are issued, it is not clear whether they fully address cyber requirements. This notwithstanding, the continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach and thus increases the risk that the nation's cyber assets have not been adequately identified, prioritized, and protected.



Results in Brief

Most sector-specific agencies developed and identified in their 2006 sector plans those actions—referred to by DHS as implementation actions—essential to carrying out the plans; however, since then, most agencies have not updated the actions and reported progress in implementing them as called for by DHS guidance. Specifically, in response to 2006 guidance that called for agencies in developing implementation actions to address three key elements (e.g., action descriptions, completion milestones), most sectors initially developed implementation actions that fully addressed the key elements; however, while 2008 guidance called for implementation actions to be updated and for sector reports to include progress reporting against implementation action milestone commitments, only five sectors updated their plans and reported on progress against implementation actions. DHS attributed this in part to the department not following up and working to ensure that all sector plans are fully developed and implemented in accordance with department guidance.



Results in Brief

The lack of complete updates and progress reports is further evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where it stands in securing its cyber and other critical infrastructure. Not following up to address these conditions also shows DHS is not making sector planning a priority. Further, the recent studies by the President's working group and expert commission also identified shortfalls in the effectiveness of the current public-private partnership approach and related sector planning and offered options for improving the process. Given this, it is essential that DHS determine whether the current process should continue to be the national approach and thus worthy of further investment

Accordingly, we are making recommendations to the Secretary of Homeland Security, consistent with any direction from the Office of the Cybersecurity Coordinator, to assess whether the existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure. If the existing approach is deemed to be the national approach, we also recommend that the Secretary make it an agency priority and manage it accordingly, including collaborating closely with other sector-specific agencies to develop (1) sector plans that fully address cyber-related criteria and (2) sector annual reports that include implementation actions and milestones and progress reporting against plan commitments and timeline.



Results in Brief

In oral and written comments on a draft of this briefing, DHS officials, including the Director of Infrastructure Protection’s Partnership and Outreach Division, which is responsible for sector-specific planning, commented on two areas. Specifically, they stated that the sector agencies had made more progress in implementing cyber-related criteria than reported in our briefing due to other ongoing DHS and sector efforts outside the sector plans and sector annual reports (implementation actions), which were the focus of the briefing. For example, DHS officials said its cyber division works regularly with many sectors on cyber assessments, exercises, and information sharing. While on the surface these may appear to improve cyber security, the officials did not show how these activities helped the agencies address missing cyber-related criteria or effectively implement their plans. The officials also said that focusing on the agencies’ efforts the year after they issued their sector plans is premature as the agencies have until 2010 to rewrite and reissue their next sector plans. This notwithstanding, DHS’s guidance calls for the sector agencies to annually review and update as appropriate their sector plans, which is a means to provide an interim snapshot of where agencies stand in addressing their gaps and is why we used it as a basis to assess progress.



Background

Consistent with the Homeland Security Act of 2002, Homeland Security Presidential Directive-7 identified

- DHS as the principal federal agency to lead, integrate, and coordinate implementation of efforts to protect critical infrastructure and key resources; and
- lead federal agencies, referred to as sector-specific agencies, as responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

It also required DHS to develop a plan that outlines national goals, objectives, milestones, and key initiatives necessary for fulfilling its responsibilities for physical and cyber critical infrastructure protection.

In 2006, DHS issued the plan—commonly referred to as the NIPP—which, in addition to addressing the above, is to serve as a road map for how DHS and other relevant stakeholders are to use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion. Further, the NIPP required the lead agencies of the 17 critical infrastructure sectors to develop a sector-specific plan (SSP) 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.



Background

In addition, as required by the NIPP, the sector-specific agencies are to provide updates on sector progress with their SSPs, including efforts to identify, prioritize, and coordinate the protection of the sector's critical infrastructure, to DHS on an annual basis. DHS is responsible for incorporating these reports into an overall critical infrastructure/key resources report, called the National Critical Infrastructure/Key Resources Protection Annual Report, which is due to the Executive Office of the President by September of each year.

Sector-specific agencies are to work in coordination with relevant government and private-sector representatives to develop and update the SSPs. Table 1 shows the designated agency for each sector.



Table 1: Designated Sector-Specific Agencies

Sector-Specific Agency	Sector
Department of Agriculture Food and Drug Administration	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Human Healthcare
Department of Homeland Security	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Government Facilities Information Technology Nuclear Reactors, Materials and Waste Postal and Shipping Telecommunication Transportation
Department of the Interior	National Monument and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water

Source: 2009 National Infrastructure Protection Plan.



Background

The sector-specific plans 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.

In addition, the plans are to identify risk management practices to be implemented, which could improve the security of the nation's cyber-reliant critical infrastructure. They also are to identify the approaches the sector will take to protect their critical cyber infrastructure.



Background

In response, the sector-specific agencies developed and issued SSPs for their sectors in May 2007. Subsequently, we examined these plans to determine the extent to which they addressed cyber security and reported⁵ in October 2007 on the extent to which the sectors addressed aspects of cyber security in their plans. Specifically, we reported that the results varied in that none of the plans fully addressed all 30 cyber security-related criteria. We also reported that 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.

Further, we recommended that DHS 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. In its October 2007 response to our report, DHS agreed with our recommendation and stated it had initiated actions to implement it.

⁵ GAO, *Critical Infrastructure Protection: Sector-Specific Plans/ Coverage of Key Cyber Security Elements Varies*, [GAO-08-113](#) (Washington, D.C.: Oct. 31, 2007).



Background

Since our 2007 report, an expert commission (led by two congressmen and industry officials) and a White House working group (established by the President) studied and reported⁶ on the public-private partnership approach and related issues such as sector planning as well as other aspects of U.S. cyber security policy. Specifically,

- In August 2007, a commission—commonly referred to as the Commission on Cybersecurity for the 44th Presidency—was established to examine the (1) adequacy of U.S. cyber strategy, including public-private partnerships and the sector approach and (2) identify areas for improvement. In December 2008, the commission reported, among other things, that the current public-private partnership and sector planning approach had serious shortcomings such as overlapping roles and responsibilities and duplication of effort. The commission made 25 recommendations aimed at addressing these and other shortfalls with the strategy and its implementation.

⁶ Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C., December 2008); and The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., May 29, 2009).



Background

- In February 2009, the President directed the National Security Council and the Homeland Security Council to conduct a comprehensive “60-day review” of all U.S. cyber policies and structures. With regard to public-private partnerships, which include sector planning, the councils reported in May 2009 that the sector and other groups involved in this area performed valuable work but that there was a proliferation of plans and recommendations that resulted in government and private sector personnel and resources being spread across a multitude of organizations engaged in sometimes duplicative or inconsistent efforts. The review concluded that there are alternative approaches for how the federal government can work with the sectors and recommended that these options be explored. At this time, the President also created the office of Cybersecurity Coordinator—who is to be part of the White House’s National Security Staff and National Economic Council—to, among other things, assist in developing a new U.S. cyber policy. The Cybersecurity Coordinator position has not yet been filled.



Results: Objective 1

Sector-Specific Agencies Have Yet to Update Their Respective Sector-Specific Plans to Fully Address Key Cyber Security Criteria as Called for by DHS Guidance

In response to our recommendation and as part of ongoing DHS efforts, the department initiated multiple efforts to improve the cyber content of their SSPs. Examples include the following:

- February 2008, DHS invited all sectors (and nine accepted) to meet with cyber experts within DHS's National Cyber Security Division to support the development of increased cyber content in SSPs.
- April 2008, DHS issued guidance to agencies on how to report on the progress of annual reviews of the SSPs.
- March 2009, DHS released guidance that specifically requested that agencies, as a part of their 2010 SSP rewrites, fully address all cyber-related weaknesses, including those identified in our October 2007 report.



Results: Objective 1

In addition to these efforts, DHS officials from the National Cyber Security Division reported that it is engaged in other activities aimed at improving, among other things, the cyber content of SSPs. They include

- working collaboratively with the sectors via a cross-sector working group⁷ to (1) analyze SSPs to identify cyber security-related gaps, (2) improve information sharing, and (3) develop measures to assess sector progress in implementing cyber security efforts;
- having personnel (from its Control Systems Security Program) lead an Industrial Control Systems Joint Working Group to foster information sharing and coordination of activities and programs across government and private sector stakeholders involved in protecting such control systems and assist with development and implementation of sector-specific control system roadmaps to secure such systems within the chemical, dams, nuclear, and water sectors by mitigating vulnerabilities;
- working with the sectors in planning and executing cyber security exercises; and

⁷ The group is called the Cross-Sector Cyber Security Working Group. It is co-chaired by DHS (National Cyber Security Division) and private sector partners. The group meets monthly and includes public and private sector security partners with cyber security expertise from each of the sectors.



Results: Objective 1

- having personnel from its Software Assurance Program work with public and private sector partners to develop a process for identifying exploitable software before security breaches occur.



Results: Objective 1

However, despite these steps, only 9 of the 17 SSPs⁸ have been updated while 8 have not.⁹

In addition, of the 9, only 3 have been revised to address missing cyber-related criteria, and those changes only involved addressing a relatively small number (3 or fewer) of missing criteria. Specifically:

- In developing the original Chemical sector SSP, DHS had fully or partially addressed 29 criteria but did not address 1. The current version of the SSP fully addressed 1 of the criteria previously assessed as partial.
- In developing the original Commercial Facilities sector SSP, DHS had fully or partially addressed 20 criteria and did not address 10. The current version of the SSP fully addressed 1 cyber-related criterion that was previously not addressed and partially addressed 1 cyber-related criterion that was previously not addressed.

⁸ Our analysis includes 17 of the 18 sectors, as the Critical Manufacturing sector was established in 2008 and has not yet finished its sector-specific plan.

⁹ While the NIPP requires SSPs to be revised and reissued every three years, it also calls for the sector-specific agencies to annually review and update as appropriate their SSPs to reflect progress on actions planned and under way. The guidance allows agencies the option to report progress via an updated plan, a list of updates, or in the case there is no progress to report, a memorandum of no action. These 8 were memorandum of no action.



Results: Objective 1

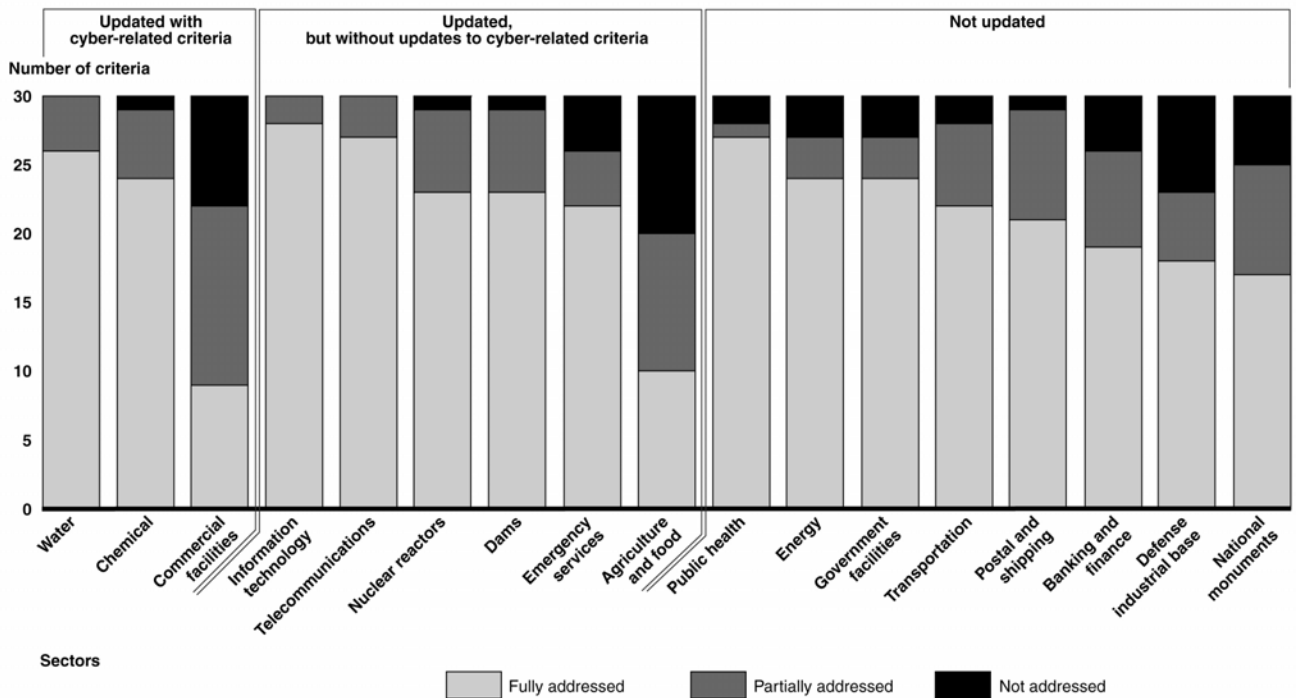
- In developing the original Water sector SSP, the Environmental Protection Agency had fully or partially addressed 29 criteria and did not address 1. The current version of the SSP fully addressed 1 cyber-related criterion that was not previously addressed and fully addressed 2 cyber-related criteria that were previously partially addressed.

Figure 1 summarizes the extent to which each SSP update addresses the 30 criteria.



Results: Objective 1

Figure 1: Sector-Specific Plan Updates



Source: GAO analysis of agency data.



Results: Objective 1

The sector-specific agencies did not fully address missing cyber-related criteria in their SSP updates in large part due to the following:

- Agency officials said that in developing their plans, they were focused more on specific (physical) threats to the sector than the cyber security aspects.
- While DHS began efforts to improve the cyber content of SSPs, sector agency officials stated that DHS did not make them aware of the specific cyber criteria shortfalls we identified and reported on in 2007.
- While DHS issued SSP (formatting) guidance in 2008, this guidance did not specifically request updates to cyber security aspects of the plans or provide other substantive-type direction.



Results: Objective 1

As previously stated, DHS issued guidance in March 2009 that specifically requested that the sectors address cyber criteria shortfalls in their 2010 sector-specific plan revisions. However, until these plans are issued, it is not clear whether they fully address cyber requirements. This notwithstanding, having sector-specific agencies continue to have SSPs that do not fully address key cyber elements has reduced the effectiveness of the existing sector planning approach and thus increases the risk that the nation's critical cyber assets have not been adequately identified, prioritized, and protected.



Results: Objective 2

Sector Plans and Related Reports Do Not Fully Provide for Effective Implementation

To provide for effective sector plan implementation, DHS issued guidance that called for the sector-specific agencies to provide for such activities in their SSPs and sector annual reports.

Specifically, with regard to the SSPs, the department issued March 2006 guidance directing the sector-specific agencies to develop and incorporate in their SSPs actions and activities—referred to as implementation actions—essential to carrying out the plans and achieving the goal of securing the sectors' cyber and other assets. According to the guidance, implementation actions are to include (1) a description of the actions necessary to implement the plan, (2) milestones for when the actions are to be accomplished, and (3) the parties responsible for managing and overseeing action execution. Developing and updating implementation actions, including milestones, and responsible parties, is important for reporting and assessing the progress and effectiveness of the sector-specific plans.



Results: Objective 2

With regard to sector annual reports, the department issued guidance in March 2008 that called for sector-specific agencies (in their 2008 annual reports to be issued later in 2008) to

- (1) update implementation actions,¹⁰ and
- (2) report on the extent of progress in achieving the actions.

¹⁰ In the 2008 guidance, DHS refers to these actions as an implementation matrix.



Results: Objective 2

Of the 17¹¹ SSPs developed in response to DHS's guidance,

- 14 included implementation actions that addressed all three elements:
 - Banking and Finance,
 - Chemical,
 - Commercial Facilities,
 - Dams,
 - Defense Industrial Base,
 - Emergency Services,
 - Government Facilities,
 - Information Technology,
 - National Monuments and Icons,
 - Nuclear Reactors,
 - Public Health and Healthcare,
 - Telecommunications,
 - Transportation, and
 - Water.
- 2 included implementation actions but each only partially addressed the three elements:
 - Energy, and
 - Postal and Shipping.

¹¹ Currently, there are 18 sectors; however, the critical manufacturing sector was established in 2008 and has not yet completed a sector-specific plan.



Results: Objective 2

Of these sectors' plans, all identified actions and milestones critical to implementation of the plan but did not identify the parties responsible for the specified actions.

- 1 did not include implementation actions:
 - Agriculture and Food.

In addition, with regard to sector annual reporting,

- 5 sectors updated and reported on the extent of progress in carrying out their implementation actions, while the other 12 did not.¹² Those that did were
 - Dams,
 - Information Technology,
 - National Monuments and Icons,
 - Nuclear Reactors,¹³ and
 - Water.

¹² The Critical Manufacturing sector was not requested to develop an annual report, as the sector was established in early 2008.

¹³ Implementation actions were updated in one area covered under the Nuclear Reactors sector.



Results: Objective 2

- Those that did not were
 - Agriculture and Food,
 - Banking and Finance,
 - Chemical,
 - Commercial Facilities,
 - Defense Industrial Base,
 - Emergency Services,
 - Energy,
 - Government Facilities,
 - Postal and Shipping,
 - Public Health and Healthcare,
 - Telecommunications, and
 - Transportation.

Figure 2 shows by sector, each sector's progress in developing and updating actions for effective implementation.



Results: Objective 2

Figure 2: Sector Progress in Developing and Updating Implementation Actions

	Agriculture & Food	Banking & Finance	Chemical	Commercial Facilities	Dams	Defense Industrial Base	Emergency Services	Energy	Government Facilities	Information Technology	National Monuments & Icons	Nuclear Reactors	Postal and Shipping	Public Health & Healthcare	Telecommunications	Transportation	Water
2007 Sector-Specific Plans																	
Elements fully addressed		X	X	X	X	X	X		X	X	X	X		X	X	X	X
Elements partially addressed								X					X				
No implementation actions	X																
2008 Annual Reports																	
Implementation actions updated					X					X	X	X					X

Source: GAO analysis of agency data.



Results: Objective 2

In addition to these implementation actions, the sectors were to report on sector goals and priorities, sector programs, sector coordination, research and development progress and gaps, funding priorities, sector security practices, and overall progress of critical infrastructure protection efforts. However, these areas, including overall progress, did not specifically address implementation progress with the sector-specific plan. For example, the energy sector reported on, among other things, progress with communicating with sector partners, protecting international energy assets, and collaborations with the Department of Homeland Security. In addition, the communications sector reported on, among other things, progress to narrow key gaps identified in the sector's 2007 report, and progress with key programs. Despite this, the reporting was not sufficient for evaluating either sector-wide progress with sector-specific plans, or the effectiveness of these plans.



Results: Objective 2

The incomplete implementation updates and progress reports are due in part to DHS not following up and working to ensure that all sector plans were fully developed and implemented in accordance with departmental guidance. Specifically, although DHS issued periodic sector-planning guidance, periodically met with sectors officials, and conducted other planning-related activities as discussed above, department officials said their follow-up and oversight of the sector plans did not always result in the sectors developing plans that fully meet DHS guidance. These officials said this occurs due to the fact that as part of DHS's partnership with the private sector, the parties do not always agree on the extent to which DHS guidance is to be addressed in performing sector planning activities. Consistent with this, our past cyber critical infrastructure protection research and extensive experience¹⁴ at the sector agencies and their private sector counterparts have shown that the public-private partnership is indeed challenging to manage. That research and work also pointed out that DHS nonetheless has a leadership role and responsibility to make sure (1) the partnership works effectively and (2) the sectors plan for and implement efforts aimed at protecting the nation's cyber and other critical infrastructure, including ensuring the current sector approach is still worth pursuing and considering, where appropriate, alternative approaches.

¹⁴ See, for example, GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434, (Washington, DC.: May 26, 2005); and *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39, (Washington, DC.: Oct. 16, 2006).



Results: Objective 2

More recently (in early 2009), DHS issued 2009 sector annual report guidance that called for the development of metrics and other implementation-related actions to, among other things, better measure progress, identify problems, and improve SSP implementation. According to responsible DHS officials, the 2009 sector reports have been drafted and provided to the department for review with the goal of incorporating a summary of these reports in DHS's national critical infrastructure protection annual report to the President by September 1, 2009. However, until DHS improves its follow-up and oversight of sector planning, effectively addresses the above-mentioned challenges of the public-private partnership, and finalizes the plans, there is increased risk that the 2009 plans will suffer from the same shortfalls as the preceding plans with the result being that sector-specific agencies will not fully and effectively report their progress in implementing their SSPs. Moreover, the incomplete implementation updates and progress reports are further evidence that the sector planning process has not been effective.



Results: Objective 2

Shortfalls with Current Public-Private Partnership Approach and Related Sector Planning Highlighted in Recent Studies by Expert Commission and Presidential Working Group

In addition to the above briefing results, the recent reports by the Commission on Cybersecurity for the 44th Presidency and President’s 60-day review also identified shortfalls with the current public-private partnership approach and relating sector planning, that show such planning is not effective. To address the shortfalls, the commission and presidential review identified options to be considered as means to improving sector planning. Examples include:

- The cyber security commission recommended simplifying the sector approach by prioritizing sectors in order to focus planning and other activities on the most important sectors—which it identified as Energy, Finance, Information Technology, and Communications—with the most important cyber assets.
- The President’s review identified a number of models of effective public-private partnership and planning (e.g., the processes and structures used by the United Kingdom) and suggested that the positive attributes of these models be applied to the sector agencies and related organizations. It also recommended streamlining existing sector and others organizations involved in the partnerships to optimize their capacity to identify priorities and develop response plans.



Conclusions

Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, the sector-specific agencies have made limited progress in updating their sector plans to fully address key cyber elements. Further, although the agencies produce extensive reports on sector activities, they have not developed effective implementation actions and reported on whether progress is being made in implementing their sector plans. This means that as a nation, we do not know precisely where we are in implementing sector plans and associated protective measures designed to secure and protect the nation's cyber and other critical infrastructure, despite having invested many years in this effort. This condition is due in part to DHS not making sector planning a priority and as such, not managing it in a way that fully meets DHS guidance. These conclusions, taken as a whole, further raise fundamental questions about whether the current approach to sector planning is worthwhile and whether there are options that would provide better results. Consequently, it is essential that federal cyber security leaders—including DHS and the to-be-appointed Cybersecurity Coordinator—exert their leadership role in this area by, among other things, determining whether it is worthwhile to continue with the current approach as implemented or consider if proposed options provide more effective results. To do less means the nation's critical infrastructure sectors will continue to be at risk of not being able to adequately protect their cyber and other critical assets or be prepared to identify and respond to cyber threats and vulnerabilities.



Recommendations for Executive Action

Accordingly, we recommend that the Secretary of Homeland Security, consistent with any direction from the Office of the Cybersecurity Coordinator, assess whether the existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure and, in doing so, consider whether proposed and other options would provide more effective results.

If the existing approach is deemed to be the national approach, we also recommend that the Secretary make it, including the cyber aspects, an agency priority and manage it accordingly. This should include collaborating closely with other sector-specific agencies to develop

- sector-specific plans that fully address cyber-related criteria in the next release of the plans, and
- sector annual reports that (1) include updated implementation actions and associated milestones and (2) report progress against plan commitments and timelines.



Agency Comments and Our Evaluation

In oral and written comments on a draft of this briefing, the Director of Infrastructure Protection's Partnership and Outreach Division and other department officials commented on the following two areas:

- First, they stated that they believed that the sector agencies had made more progress in implementing cyber-related criteria than reported in our briefing due to other ongoing DHS and sector efforts outside the SSPs and sector annual reports (implementation actions), which were the focus of the briefing. For example, DHS officials said its National Cyber Security Division works regularly with many sectors on cyber assessments, exercises, and information sharing. In addition, DHS cites two cross-sector cyber working groups that play an important role in advancing cyber security. While these and the other examples provided by DHS on the surface appear to improve cyber security, DHS officials did not show how these activities helped the agencies address missing cyber-related criteria in their SSPs or effectively implement their plans.



Agency Comments and Our Evaluation

- Second, the officials stated that focusing on the agencies' efforts the year after they issued their sector plans is premature as the agencies have until 2010 to rewrite and reissue their next sector plans. While the NIPP calls for the next SSPs to be issued in 2010, it also calls for the sector-specific agencies to annually review and update as appropriate their SSPs, which is a means to provide an interim snapshot of where agencies stand in addressing their gaps and is why we used it as a basis to assess agency progress.

DHS officials also provided technical comments, which we have incorporated into the briefing as appropriate.



Attachment I
Scope and Methodology

Attachment I: DHS's Cyber Criteria Organized by Major Reporting Sections

<p>Section 1: Sector Profile and Goals</p> <ul style="list-style-type: none">• Characterizes cyber aspects• Identifies stakeholder relationships for securing cyber assets <p>Section 2: Identify Assets, Systems, Networks, and Functions</p> <ul style="list-style-type: none">• Describes process to identify cyber assets, functions, or elements• Describes process to identify cyber dependencies/independences <p>Section 3: Assess Risks</p> <ul style="list-style-type: none">• 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 <p>Section 4: Prioritizing Infrastructure</p> <ul style="list-style-type: none">• Identifies entity responsible for prioritization of cyber aspects• Describes criteria and basis for prioritization of cyber aspects <p>Section 5: Develop and Implement Protective Programs</p> <ul style="list-style-type: none">• 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	<p>Section 6: Measure Progress</p> <ul style="list-style-type: none">• 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 <p>Section 7: Critical Infrastructure Protection Research and Development (R&D)</p> <ul style="list-style-type: none">• 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 <p>Section 8: Managing Sector-Specific Agency Responsibilities</p> <ul style="list-style-type: none">• 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 of DHS's SSP guidance.

Appendix II: Comments from the Department of Homeland Security

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



**Homeland
Security**

September 11, 2009

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

Dear Mr. Powner:

RE: Draft Report GAO 09-969 (Reference # 310891) Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment

Thank you for the opportunity to review the draft report concerning critical infrastructure protection. In addition to responding to the recommendations in the Government Accountability Office's (GAO's) draft report, we are providing general comments that address what we believe are errors, misinterpretations, and incorrect conclusions contained in the text of the report and the appendix.

Recommendation: "GAO recommends the Secretary of DHS, consistent with any direction from the Office of Cybersecurity Coordinator, assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure and, in doing so, consider whether proposed or other options would provide more effective results.

If the existing approach is deemed to be the national approach, we also recommend that the Secretary make it, including the cyber aspects, an agency priority and manage it accordingly. This should include collaborating closely with other sector-specific agencies to develop

- sector-specific plans that fully address cyber-related criteria in the next release of the plans, and
- sector annual reports that (1) include updated implementation actions and associated milestones and (2) report progress against plan commitments and timelines"

Response: The Department of Homeland Security (DHS) supports the ongoing assessment and improvement of the sector planning approach. DHS continually assesses the effectiveness of this approach and identifies and implements improvements. However, DHS does not concur with some of the conclusions stated in the draft report, which form the basis

for GAO's recommendations (see below) and which relate to updates to Sector-Specific Plans (SSPs) and implementation actions in the Sector Annual Reports. The draft report does not give due consideration to many of the ongoing sector and cross-sector cybersecurity activities identified in the annual reports and briefed to GAO.

If the recommendation is intended to suggest that there is a binary choice between continuing the existing sector-specific planning approach and other options, DHS disagrees; actions such as prioritization of efforts with or among sectors and use of supplemental approaches (for example, certain planning requirements relevant to cybersecurity are mandatory for parts of the chemical sector) can move forward in parallel with ongoing sector-planning activity. And as stated above, DHS believes we must continue to refine our work with the private sector regarding cybersecurity to enhance the effectiveness of our partnerships. As stated in the Cyberspace Policy Review:

Partnerships must evolve to clearly define the nature of the relationship, the roles and responsibilities of various groups and their participants, the expectations of each party's contribution, and accountability mechanisms. The Federal government should streamline, align, and provide resources to existing organizations to optimize their capacity to identify priorities, enable more efficient execution, and develop response and recovery plans.

The efforts of DHS, and of the Federal government, to implement this recommendation are ongoing.

Finally, as discussed in General Item 5 of our comments, the report confuses elements of the planning and reporting processes under the National Infrastructure Protection Plan (NIPP), leading to inaccurate conclusions.

General Comments

General Item: 1; Page: 3

Issue: "Sector-Specific Agencies have yet to update their respective Sector-Specific Plans to fully address key cybersecurity criteria as called for by DHS guidance."

DHS Statement: The risk management framework outlined in the 2006 NIPP established the process for combining consequence, vulnerability, and threat information to produce a comprehensive and systematic assessment of national and sector-specific risk that drives Critical Infrastructure and Key Resources (CIKR) protection activities. At each step of the risk management framework, the physical, cyber, and human elements of CIKR are considered. The 2006 guidance for developing the SSPs was based on this NIPP risk management framework and its consideration of all three elements of CIKR. The 2006 SSP guidance did not call for the cyber element to be addressed separately in each section of the SSP; GAO had not identified the 30 cybersecurity criteria at that time. The GAO's 30 cybersecurity criteria were therefore not fully addressed in the 2007 SSPs; however, the physical, cyber, and human elements of CIKR were considered and addressed by each of the individual sectors, in accordance with DHS guidance.

In accordance with the NIPP, the NIPP and the SSPs are reviewed on an annual basis for currency and continued relevance to all CIKR partners. The sectors issue SSP Updates as

deemed necessary based on the annual review of their SSPs. Nine Sector-Specific Agencies (SSAs) issued 2008 Updates to their SSPs. In 2008, DHS also conducted a comprehensive triennial review and update of the NIPP. Released in early 2009, the revised NIPP captures the evolution and maturation of the processes and programs first outlined in 2006, including more robust coverage of cybersecurity, based on the 30 cyber criteria identified by GAO.

The SSAs are currently conducting a comprehensive triennial review and rewrite of their SSPs for reissue in 2010. DHS' guidance for the 2010 SSP rewrites is based on the updated 2009 NIPP and incorporates GAO's cyber criteria. The 2010 SSPs will address cybersecurity more completely based on DHS guidance and a prioritization of risk within each sector.

General Item: 2; Page: 4

Issue Summary: Sector-specific agencies did not fully address missing cyber criteria in their plans in part because "they were unaware of the cyber criteria shortfalls identified in 2007."

DHS Statement: DHS approached SSAs through multiple avenues to bring the 2007 GAO report to their attention. The National Cyber Security Division (NCSD) invited the SSAs to meet with subject-matter experts regarding their SSPs and Sector Annual Reports. The agenda for the initial meetings included discussion of the 2007 GAO findings. In addition, NCSD worked collaboratively with public and private partners from the sectors through the Cross-Sector Cyber Security Working Group (CSCSWG) to assist them in analyzing and identifying gaps in their respective SSPs and Sector Annual Reports.

General Item: 3; Page: 4

Issue: "The lack of complete updates and progress reports are further evidence that the sector planning process has not been effective and thus leaves the Nation in a position of not knowing precisely where we stand in securing cyber critical infrastructures."

DHS Statement: The fact that all the SSPs have not been fully updated yet to include ongoing and planned cybersecurity activities does not correlate to a lack of cybersecurity planning and activities in the sectors or to the lack of effectiveness of planning, nor has GAO demonstrated this correlation in the draft report. The report also does not take into account the many ongoing activities in the sectors related to cybersecurity. These activities are described below. Additionally, all the sectors reported on their CIKR protection progress in the 2008 Sector Annual Reports.

General Item: 4; Page: 5

Issue: "Although DHS reported many efforts underway and planned to improve the cyber content of sector-specific plans, sector-specific agencies have yet to update their plans to fully address key DHS cybersecurity criteria. The continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach."

DHS Statement: GAO expanded the scope of this engagement beyond the initial focus on coverage of cybersecurity in the SSPs to encompass the entire sector planning approach. DHS was not asked to provide a broader update on the NIPP public-private partnership, and

the draft report does not include information previously provided by DHS on the numerous ongoing partnership activities specifically related to cybersecurity, such as:

- The CSCSWG, co-chaired by NCSA and private-sector representatives, meets on a monthly basis to address a broad range of cyber-related issues in addition to the SSPs and Sector Annual Reports. The CSCSWG includes public- and private-sector partners with cybersecurity expertise from the CIKR sectors and their SSAs. NCSA's Critical Infrastructure Protection Cybersecurity Program is providing cybersecurity expertise in support of an initiative within the CSCSWG to develop cybersecurity measures for all 18 CIKR sectors.
- NCSA provides assistance to the Transportation, Critical Manufacturing, Commercial Facilities, Chemical, Banking & Finance, and Defense Industrial Base (DIB) Sectors and their SSAs in support of the sectors' broader cybersecurity activities, including risk management (e.g., the DIB Sector's Cybersecurity Task Force).
- NCSA's Control Systems Security Program leads the Industrial Control Systems Joint Working Group (ICSJWG) to foster information sharing and coordination of activities and programs across government and private-sector stakeholders involved in protecting CIKR. The ICSJWG is a collaborative coordinating body that provides a vehicle for communicating and partnering between Federal agencies and private asset owner/operators of industrial control systems.
- NCSA manages the United States Computer Emergency Readiness Team (US-CERT), which has monthly situational awareness conference calls with the Information Technology Information Sharing and Analysis Center (ISAC), Financial Services ISAC, Multi-State ISAC, and members of the Chemical Sector, through the NIPP partnership framework.
- During significant events, US-CERT holds conference calls with the private sector regarding recent threats and vulnerabilities and associated mitigation activities through the CSCSWG and ISAC Council distribution.

Additionally, during the week of August 24, 2009, a public-private risk assessment of the Information Technology Sector was issued jointly by the IT Sector Coordinating Council and Government Coordinating Council. The Energy Sector recently completed work on a joint public-private Control Systems Roadmap Update, which it plans to issue in the next few months. The framework of trusted relationships built through the NIPP sector partnership is essential to the development of these joint products. The partnership framework continues to evolve and improve, using shared lessons learned across and between all sectors.

General Item: 5; Appendix I, slide 14

Issue: "DHS guidance calls for the sector agencies to annually review and update as appropriate their sector plans, which is a means to provide an interim snapshot of where agencies stand in addressing their gaps and is why we used it as a basis to assess progress."

DHS Statement: The SSP is a strategic, three-year plan and is not meant to provide a snapshot of where agencies stand in addressing their gaps, nor should it be used as a basis to

assess progress in CIKR protection. The Sector Annual Report serves these purposes. The NIPP calls for the sector-specific agencies to review their SSPs on an annual basis and issue updates, as needed, to capture changes in sector programs and processes and maintain currency for all sector partners.

General Item: 6; Page: 4

Issue: "Most sector-specific agencies developed and identified in their 2007 sector plans those actions—referred to by DHS as implementation actions—essential to carrying out the plans; however, since then, most agencies have not updated the actions and reported progress in implementing them as called for by DHS guidance."

DHS Statement: Implementation actions were identified in DHS' 2006 SSP guidance for the development of the 2007 SSPs; many of the implementation actions were one-time actions that were completed in 2007 or 2008. Others are of an ongoing, continuous nature. In 2008, sectors were asked to review these items and incorporate new and ongoing activities for which progress could be measured. All the sectors reported on their CIKR protection progress in the 2008 Sector Annual Reports; however only some included actual implementation action matrices. Since the vast majority of these items were completed, DHS made adjustments in 2009 to the reporting process to better reflect the maturation of the sectors and more accurately capture the progress of CIKR protection efforts. DHS is now working with the sectors toward the development of outcome metrics designed to measure the beneficial value of activities in mitigating risks to CIKR.

General Item: 7; Page: 5

Issue: "Not following up to address these conditions also shows DHS is not making sector planning a priority."

DHS Statement: DHS is actively engaged with the SSAs and sectors regarding the implementation of the NIPP. DHS assists the sectors with planning and reporting on an ongoing basis and continually evaluates and improves these processes, with input from the sectors.

General Item: 8; Pages: 2, 3; Appendix I, slide 39

Issue Summary: An expert commission and the President's cybersecurity working group conducted studies on cybersecurity and the public-private partnership; both studies identified issues with the current sector planning approach.

DHS Statement: GAO did not discuss or reference these studies with DHS' Office of Infrastructure Protection.

General Item: 9; Page: 6

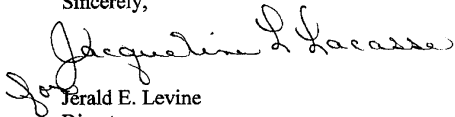
Issue: "This should include collaborating closely with other sector-specific agencies to develop sector-specific plans that fully address cyber-related criteria in the next release of the plans."

**Appendix II: Comments from the Department
of Homeland Security**

DHS Statement: This effort is well underway as part of the ongoing rewrite of the SSPs for reissuance in 2010.

Again, thank you for the opportunity to comment on this Draft Report and we look forward to working with you on future homeland security issues.

Sincerely,


Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, the following staff also made key contributions to this report: Gary Mountjoy, Assistant Director; Scott Borre; Rebecca Eyler; Lori Martinez; and Teresa Smith.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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