United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2009

CRITICAL INFRASTRUCTURE PROTECTION

OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets

GAO-10-148

October 2009

CRITICAL INFRASTRUCTURE PROTECTION

OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-148, a report to congressional requesters

Why GAO Did This Study

Because the nation's critical infrastructure relies on information technology systems and data, the security of those assets is critical to ensuring national security and public safety. In 2003, the President directed federal agencies to (1) develop plans for the protection of their computer-related (cyber) critical infrastructure assets and (2) submit them for approval to the Office of Management and Budget (OMB) by July 31, 2004. To help agencies do this, OMB issued guidance with 19 criteria deemed essential for effective cyber critical infrastructure protection planning that were required to be included in the plans. GAO was asked to determine (1) the extent to which agencies developed their plans and whether they submitted them to OMB by the deadline and (2) whether the plans met criteria in OMB's guidance. To do this, GAO reviewed plans from 24 agencies, many of which own and operate key government cyber and other critical infrastructure; reviewed OMB documentation; interviewed officials; and compared submitted plans to relevant criteria

What GAO Recommends

GAO is recommending that OMB (1) direct agencies to update cyber plans to fully address OMB requirements and (2) follow up to see that agencies make sure plans meet requirements and are being implemented. In commenting on a draft of this report, OMB agreed with the first recommendation; it agreed with the second after GAO revised it to better clarify OMB and agency follow up responsibilities.

View GAO-10-148 or key components.
For more information, contact Dave Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Key federal agencies developed and submitted cyber critical infrastructure protection plans or related documentation to OMB in response to the President's direction (Homeland Security Presidential Directive 7) and associated OMB guidance. Specifically, of the 24 agencies, 18 submitted plans, while the remaining 6, as allowed by the guidance, provided documentation in lieu of plans stating that they neither owned nor operated any of the nation's cyber critical infrastructure. The agencies submitted their plans and documentation to OMB by the July 31, 2004, deadline.

Agencies' plans, in large part, did not fully address the 19 cyber and related requirements specified in OMB's guidance. Specifically, only 4 of the 18 plans fully addressed all the criteria. While the other 14 plans fully addressed at least 8 or more criteria, they only partially addressed or did not address others—such as prioritizing key assets and documenting a strategy to protect them—that are essential for effectively planning for the protection of cyber assets. Since the development of these plans, 8 agencies whose plans did not fully meet OMB's criteria have engaged in other critical infrastructure protection planning and related efforts that addressed some, but not all, of their shortfalls.

The shortfalls in meeting OMB's guidance are attributable, in part, to OMB not making these plans a priority and managing them as such by, for example, following up on a regular basis to assess whether agencies are updating their plans to fully address the requirements and are effectively implementing them. When agencies submitted their initial plans, OMB reviewed and provided feedback on their adequacy, but did not follow up to verify that agencies had revised their plans to incorporate OMB feedback or to determine whether planning was being implemented and institutionalized. OMB attributed this to its attention being focused on other competing issues. In addition, OMB did not direct agencies to periodically update their plans. Without more sustained leadership, management, and oversight in this area, there is an increased risk that federal agencies individually, and the federal government collectively, will not effectively identify, prioritize, and protect their critical cyber assets, leaving them vulnerable to efforts to destroy, incapacitate, or exploit them.

Contents

Abbreviations

CIP	critical infrastructure protection
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of Interior
DOJ	Department of Justice
DOT	Department of Transportation
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
HHS	Health and Human Services
HSPD-7	Homeland Security Presidential Directive 7
IT	information technology
NASA	National Aeronautics and Space Administration
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SBA	Small Business Administration
SSA	Social Security Administration
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 15, 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 Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security and Infrastructure Protection
Committee on Homeland Security
House of Representatives

The Honorable James R. Langevin
House of Representatives

Because the nation's critical infrastructure[1] relies extensively on computerized information technology (IT) systems and electronic data, the security of those systems and data is essential to our nation's security, economy, and public health and safety. Providing continuity of government requires ensuring the safety of the government's own critical computer-related (cyber) infrastructure and assets that are essential to support key missions and services.

To address increasing threats to the cyber infrastructure and assets of the federal government, the President, in December 2003, issued Homeland Security Presidential Directive 7 (HSPD-7), which called for federal departments and agencies to identify, prioritize, and protect the United States' critical infrastructure and key resources[2] (hereafter referred to as "critical infrastructure"). Specifically, HSPD-7 required, among other things, that federal departments and agencies develop and submit to the

[1]Critical infrastructure means IT and non-IT systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these.

[2]Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government (e.g., nuclear power plants, and certain dams, government facilities, and commercial facilities).

Office of Management and Budget (OMB) for approval, plans for protecting the cyber and other (e.g., physical) critical infrastructure that they own or operate. HSPD-7 also required that these plans (1) address identification, prioritization, protection, and contingency planning, including recovery of essential capabilities and (2) be submitted to OMB by July 31, 2004.

To aid federal agencies in this effort, OMB issued a memorandum in June 2004 (referred to as M-04-15), instructing agencies on how these plans were to be developed. The directive also included 19 criteria OMB deemed essential for preparing an effective cyber critical infrastructure protection (CIP) plan that were required to be included in the plans. While these plans are key to protecting federally owned or operated critical infrastructure, OMB stated that another goal of the plans was to initiate and, ultimately, institutionalize cyber CIP planning across the federal government.

This report responds to your request that we determine (1) the extent to which federal agencies have developed plans for protecting their cyber critical infrastructure and whether they have submitted them to OMB, as required by HSPD-7, and (2) whether the submitted plans met the criteria in OMB's instructions and related guidance. To carry out these objectives we, among other things, requested and reviewed the cyber critical infrastructure plans and related documentation of 24 major executive branch agencies,[3] reviewed OMB documentation, and interviewed OMB officials. We compared the plans against the 19 cyber-related criteria contained in OMB's M-04-15 memorandum to determine whether they fully addressed, partially addressed, or did not address the criteria. We interviewed agency officials to verify our understanding of their plans and to validate the accuracy of our analysis; in cases where agencies stated that they owned no nationally critical cyber infrastructure, we reviewed documentation submitted to OMB in lieu of a plan to assess its reasonableness.

[3]These are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

We performed this performance audit in the Washington, D.C., metropolitan area 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.

On September 3, 2009, we briefed your staffs on the results of our review. This report summarizes and transmits the (1) presentation slides we used to brief the staff and (2) recommendations to the Director of OMB that are part of those slides. The full briefing materials, including details on our scope and methodology, are reprinted as appendix I.

In summary, we made the following major points:

- Major federal agencies developed and submitted cyber CIP plans or related documentation to OMB in response to HSPD-7 and associated OMB instructions. Specifically, of the 24 major agencies, 18 submitted plans; the remaining 6, as allowed by the directives, provided documentation in lieu of plans, stating that they neither owned nor operated any of the nation's cyber critical infrastructure. The agencies submitted their plans and documentation to OMB by the July 31, 2004, deadline.

- Agencies' initial plans largely did not fully address the 19 cyber and related requirements specified in OMB's instructions. Specifically, only 4 of the 18 plans fully addressed all the criteria. While the other 14 plans fully addressed at least 8 or more criteria, they only partially addressed or did not address others—such as prioritizing key assets and documenting a strategy to protect them—that are essential to effectively plan for the protection of cyber assets. In addition, the agencies have not updated their plans since 2004. However, 8 agencies whose plans did not fully meet OMB's criteria have engaged in other CIP planning and related efforts that addressed some, but not all, of their shortfalls.

- The shortfalls in meeting OMB's guidance are attributable, in part, to the fact that OMB has not made these plans a priority and managed them as such by, for example, following up on a regular basis to assess whether agencies have updated their plans to fully address OMB requirements and are effectively implementing them. When agencies submitted their initial plans, OMB reviewed them and provided feedback on their adequacy, but did not follow up to verify that agencies had revised their plans to

incorporate OMB feedback or to determine whether planning was being implemented and institutionalized. OMB attributed this to its attention being focused on other, competing issues. In addition, OMB did not direct agencies to periodically update their plans.

Conclusions

The major federal agencies' 2004 cyber CIP plans were an initial step toward the goals of (1) securing and protecting critical infrastructure and assets vital to carrying out the government's mission-critical operations and (2) implementing and institutionalizing cyber CIP planning governmentwide. While none of the 2004 plans have since been updated, subsequent cyber CIP planning efforts by one-third of the agencies have yielded additional steps toward these goals. However, continuing shortfalls in these planning efforts highlight that more remains to be done to ensure cyber CIP plans are developed in a comprehensive manner. These shortfalls are attributable, in part, to OMB not making these plans a priority, including not effectively overseeing agencies' efforts to make sure OMB requirements are addressed in agency plans and the plans are being implemented. Without more sustained leadership, management, and oversight in this area, there is an increased risk that federal agencies individually, and the federal government collectively, will not, among other things, effectively identify, prioritize, and protect their cyber critical assets, thus leaving them potentially vulnerable to deliberate efforts to destroy, incapacitate, or exploit them.

Recommendations for Executive Action

We are recommending that the Director of OMB provide leadership and oversight in directing federal cyber critical infrastructure planning efforts and make them a management priority by

- directing the federal agencies to expeditiously update their plans to fully address OMB's cyber critical infrastructure planning requirements, and
- following up, as appropriate, to see that agencies are making sure updated plans fully meet OMB requirements and are being effectively implemented. At a minimum, this should include having agency heads report to OMB when updated plans have been completed and that the plans fully meet OMB requirements and are being effectively implemented.

Agency Comments and Our Evaluation

In oral comments on a draft of this report—which were provided by the Lead Information Technology Policy Analyst from the Office of E-Government and Information Technology—OMB agreed with our findings and first recommendation and discussed issuing a clarifying memorandum

to direct agencies to update their plans. With regard to our second recommendation, OMB agreed with it in principle but expressed concern that the recommendation (as worded in the draft) would be interpreted to mean that OMB is solely responsible for following up when it is a key responsibility of the agencies to follow up to make sure their plans are effectively updated and implemented. We concur that agencies have a key role to play in updating and implementing these plans due to their intimate knowledge of their respective cyber CIP environments and, therefore, know how best to secure and protect them. To better clarify OMB and agency responsibilities, we slightly revised the second recommendation, and OMB agreed with it as reworded. This revision does not change the fact that OMB, as discussed in this report and in our presentation slides, also has an important role to play in periodically following up with the agencies to, among other things, assess the status and progress of their cyber CIP planning efforts.

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, OMB, 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.

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

David A. Powner
Director, Information Technology Management Issues

Appendix I: Briefing to Staff of Congressional Committees

Critical Infrastructure Protection: OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets

Briefing for Staff Members of the

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

House Committee on Homeland Security

and the

Subcommittee on Transportation Security and Infrastructure Protection

House Committee on Homeland Security

August 27, 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

2

Introduction

Because the nation's critical infrastructure[1] relies extensively on computerized information technology (IT) systems and electronic data, the security of those systems and information is essential to our nation's security, economy, and public health and safety. Providing continuity of government requires ensuring the safety of the government's own cyber infrastructure and assets that are essential to supporting key missions and services.

In particular, the cyber infrastructure and assets of the federal government are under an increasing threat. U.S. intelligence officials have stated publicly that, as the government continues to move to network operations, the threat to these systems will continue to grow. These officials have also commented that nation-states and criminals target federal and other sectors' IT networks to gain commercial competitive advantage and terrorist groups have expressed the desire to do the same as a means of attacking the United States.

[1] Critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.

3

Introduction

To address these threats, the President, in December 2003, issued Homeland Security Presidential Directive 7 (HSPD-7), which called for federal departments and agencies to identify, prioritize, and protect the United States' critical infrastructure and key resources[2] (hereinafter referred to as "critical infrastructure"). Specifically, HSPD-7 required, among other things, that federal departments and agencies develop and submit to the Office of Management and Budget (OMB) plans for protecting the cyber and other (e.g., physical) critical infrastructure that they own or operate. The presidential directive also required that these plans

(1) address identification, prioritization, protection, and contingency planning, including recovery of essential capabilities and

(2) be submitted to OMB by July 31, 2004.

To aid federal agencies in this effort, OMB issued a memorandum in June 2004 (referred to as Memorandum M-04-15) instructing agencies on how these plans were to be developed; the directive also included 19 cyber and related criteria to be addressed that OMB deemed essential to preparing an effective cyber protection plan.

[2] Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government. Examples include such facilities as nuclear power plants, dams, government facilities, and commercial facilities.

4

Objectives, Scope, and Methodology

As requested, our objectives were to determine

- the extent to which federal agencies have developed plans for protecting their cyber critical infrastructure and whether they have submitted them to OMB as required by HSPD-7, and
- whether the submitted plans met the criteria in OMB's instructions and related guidance.

5

Objectives, Scope, and Methodology

For objective 1, we contacted 24 major executive branch departments and agencies[3] to request their cyber critical infrastructure protection (CIP) plans submitted to comply with HSPD-7 and OMB memorandum M-04-15. We focused on these agencies because they own and operate key cyber and other critical infrastructure essential to carrying out the government's mission-critical functions. We also reviewed OMB documentation and interviewed OMB officials to confirm which federal agencies had submitted CIP plans as required.

[3]These are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and the U.S. Agency for International Development.

6

Objectives, Scope, and Methodology

For objective 2, we analyzed OMB's M-04-15 memorandum and identified the 19 cyber and related criteria that agencies were to use in developing their plans. These criteria, taken as a whole, called for the agencies to address the following key topics: whether the agencies had (1) existing capabilities, including dedicated human capital and funding resources, to protect their cyber critical infrastructure assets, (2) a prioritized inventory of such assets, and (3) a documented strategy to protect them. (See slides 19-20 for the 19 criteria organized by these key topics.) We then analyzed the plans of the 24 major agencies using the 19 criteria to determine whether there were variances. If there were, we reviewed documentation and interviewed appropriate agency officials to identify causes and any impacts. In analyzing the plans against the 19 criteria, we used the following categories to describe the extent to which the plans addressed each criterion:

- fully addressed: the plan specifically addressed the criterion
- partially addressed: the plan addressed some but not all parts of the criterion
- not addressed: the plan did not specifically address the criterion

7

Objectives, Scope, and Methodology

Further, we also interviewed responsible agency officials to, among other things, verify our understanding of their cyber and related plans and to validate the accuracy of our analyses of the extent to which the criteria had been addressed in the plans. For agencies stating that they owned no nationally critical cyber infrastructure, we reviewed documentation they submitted to OMB (in lieu of a report) to assess its reasonableness.

We conducted this performance audit in the Washington, D.C., metropolitan area from October 2008 to June 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.

8

Results in Brief

Major federal agencies developed and submitted cyber critical infrastructure protection plans or related documentation to OMB in response to HSPD-7 and associated OMB instructions. Specifically, of the 24 major agencies,18 submitted such plans; the remaining 6, as allowed by the directives, provided documentation—in lieu of a detailed plan—stating that they neither owned nor operated any of the nation's cyber critical infrastructure. The agencies submitted their plans and documentation to OMB by the July 31, 2004, deadline specified in the directives.

In developing their initial plans, the agencies in large part did not fully address the 19 cyber and related requirements specified in OMB's instructions. Specifically, only 4 of the 18 plans submitted to OMB fully addressed all criteria. In addition, while the other 14 plans fully addressed at least 8 or more criteria, they only partially addressed or did not address at all other criteria—such as including a prioritized inventory of cyber critical infrastructure assets and a documented strategy to protect them—that are essential to effectively planning for the protection of cyber assets. For example, four agencies did not include a cyber critical infrastructure asset inventory, and eight did address whether they had a cyber protection strategy. Since the development of these plans, eight agencies—whose plans did not fully meet OMB requirements—have engaged in other CIP planning and related efforts that addressed some but not all of their OMB requirement shortfalls.

9

Results in Brief

The shortfalls in meeting OMB's requirements are attributable in part to the fact that OMB has not made these plans a priority and managed them as such by, for example, following up on a regular basis to assess whether agencies are updating their plans to fully address the requirements and are effectively implementing them. OMB attributed this to its attention being focused on other competing issues. When agencies submitted their initial plans, OMB reviewed and provided feedback on the adequacy of the plans but did not follow up to verify that the agencies had revised the plans to incorporate OMB's feedback or to determine whether the planning was being implemented and institutionalized. Until these shortfalls are fully addressed, there is an increased risk that the federal government will not effectively identify, prioritize, and protect its cyber critical assets, leaving them potentially vulnerable to deliberate efforts to destroy, incapacitate, or exploit them.

To address this risk, it is essential that OMB provide sustained leadership, management, and oversight in this area. Accordingly, we are recommending that the Director of OMB, among other things, provide this level of management effort in directing federal cyber critical infrastructure planning and make such planning a priority by (1) directing the agencies to update their cyber plans to fully address OMB requirements and (2) following up as appropriate to make sure updated plans meet requirements and that the plans are being effectively implemented.

10

Results in Brief

In oral comments on a draft of this briefing, OMB officials, including the Lead Information Technology Policy Analyst from the Office of E-Government and Information Technology, agreed with our findings and first recommendation and discussed issuing a clarifying memorandum to direct agencies to update their plans. With regard to our second recommendation, these officials said that it was ultimately the responsibility of the agencies to follow up to make sure plans are updated and implemented. We agree that the agencies have a key role to play in these planning efforts. We also believe OMB plays an important and unique role in that it is responsible for reviewing and approving agency plans across the entire federal government. To do this effectively, OMB should periodically follow up with the agencies to assess status and progress of cyber CIP planning efforts.

11

Background

Increased Vulnerabilities Could Expose Federal Systems to Attack

As federal IT systems increase their connectivity with other networks and the Internet and as their system capabilities continue to increase, these systems will become increasingly vulnerable. For example, we reported[4] in 2008 that the National Vulnerability Database, the U.S. government repository of standards-based vulnerability management data, had gathered information on the growing problem, including the following:

- About 29,000 security vulnerabilities or software defects exist that can be directly used by a hacker to gain access to a system or network.
- On average, close to 18 new vulnerabilities are added to the database each day.
- More than 13,000 software products contain security vulnerabilities.

These vulnerabilities become particularly significant when considering the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. Thus, protecting federal IT systems and the systems that support critical infrastructures has never been more important.

[4] GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, DC.: March 12, 2008).

12

Background
Past GAO Work

We have previously reported[5] on agency efforts to protect their IT systems, including meeting Federal Information Security Management Act (FISMA)[6] requirements and requirements for federal continuity of operations planning. We found that federal agencies have made progress in strengthening information security, as required by FISMA. However, most agencies continue to experience significant deficiencies that jeopardize the confidentiality, integrity, and availability of their systems and information. A primary reason for these problems is that agencies have not fully institutionalized comprehensive security management programs. We recently highlighted these issues in our 2009 High Risk report.[7]

[5] See, for example, GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses,* GAO-09-546 (Washington, DC.: July 17, 2009); *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, DC.: March 12, 2008); and *Continuity of Operations: Selected Agencies Tested Various Capabilities during 2006 Governmentwide Exercise*, GAO-08-185 (Washington, D.C.: November 19, 2007).

[6] Title III, E-Government Act of 2002, Pub. L. No. 107-347.

[7] GAO, *High-Risk Series, An Update*, GAO-09-271 (Washington, D.C. : January 2009).

Background

In December 2003, the President issued HSPD-7, which called for federal departments and agencies to identify, prioritize, and protect the United States' critical infrastructure and key resources.[8] Specifically, HSPD-7 required, among other things, that federal departments and agencies develop and submit to OMB plans for protecting the cyber and other (e.g., physical) critical infrastructure that they own or operate. The presidential directive also required that these plans (1) address identification, prioritization, protection, and contingency planning, including recovery of essential capabilities and (2) be submitted to OMB by July 31, 2004.

To help in the development of the plans, OMB issued a directive (Memorandum 04-15, dated June 17, 2004 and signed by OMB's director) that instructed the departments and agencies on how the plans were to be developed and reiterated the July 31, 2004, deadline for plan submission to OMB. The memorandum also stated that agencies that determined that they did not have cyber and other critical infrastructures were still required to report this to OMB by the specified dateline.

[8] Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government. Examples include such facilities as nuclear power plants, dams, government facilities, and commercial facilities.

14

Background

While these plans are key to protecting federally owned or operated critical infrastructure, they are also intended to be an important input for the Department of Homeland Security (DHS) to use in developing the National Infrastructure Protection Plan, a plan DHS first developed in 2006 to establish national priorities, goals, and requirements for CIP. The National Infrastructure Protection Plan was to then outline the methodology for determining which government facilities are priorities for protection. Further, OMB officials stated that another goal of these plans was to initiate, and ultimately institutionalize, cyber CIP planning across the federal government.

15

Results: Objective 1

All major federal agencies developed and submitted cyber CIP plans or related documents to OMB

The 24 major agencies developed and submitted cyber CIP plans or related documents in response to HSPD-7 and OMB requirements. The agencies submitted their plans and documentation to OMB by the July 31, 2004, deadline specified in these directives.

- The following 18 agencies submitted plans to address protecting their cyber critical infrastructures:
  - Agriculture
  - Commerce
  - Defense
  - Energy
  - Environmental Protection Agency
  - Health and Human Services
  - Homeland Security
  - Interior
  - Justice
  - Labor
  - National Aeronautics and Space Administration
  - Office of Personnel Management
  - Small Business Administration
  - Social Security Administration
  - State
  - Transportation
  - Treasury
  - Veterans Affairs

16

Results: Objective 1

- These remaining 6 agencies submitted documentation (e.g., memorandum) stating that they neither owned nor operated cyber infrastructure critical to the nation:
  - Education
  - General Services Administration
  - Housing and Urban Development
  - National Science Foundation
  - Nuclear Regulatory Commission
  - U.S. Agency for International Development

  In reviewing the documentation submitted by these agencies, it appears the agencies' statements that they had no cyber critical infrastructures are reasonable based on the evidence they provided.

17

Results: Objective 2

Initial agency plans in large part did not fully address OMB's cyber CIP planning requirements, and while subsequent agency planning efforts addressed some requirement shortfalls, they did not address others essential to effective planning

In instructing the departments and agencies on how their plans were to be developed, OMB's directive specified 19 cyber and related CIP planning requirements essential to each agency in developing its plan. Taken collectively, these criteria called for agencies to address the following key topics: whether they had (1) existing capabilities, including dedicated human capital and funding resources, to protect their cyber critical infrastructure assets; (2) a prioritized inventory of such cyber assets; and (3) a documented long-term strategy to protect them, including metrics to measure cyber program performance. The 19 criteria, grouped by key topic area, are described on the following slides. Once completed, these plans were intended to be a blueprint for how agencies are to protect their cyber and other critical infrastructure, serve as input into the National Infrastructure Protection Plan, and initiate cyber CIP planning across the federal government.

18

Results: Objective 2

OMB Memorandum 04-15 cyber and related CIP planning criteria

Addressing existing capabilities for protecting federal cyber critical infrastructure

- Summarize primary functions of the agency that rely on cyber critical infrastructure assets
- Summarize the agency's management structure, including the management responsible for the security of cyber critical infrastructure assets
- Summarize locations and assets that support the primary functions
- Describe the agency's current capabilities for identification of federally owned or operated cyber critical infrastructure assets
- Describe the agency's current capabilities for assessments of cyber vulnerabilities and interdependencies
- Describe the agency's current capabilities for prioritization of federal cyber assets
- Describe the agency's current capabilities for adequately protecting cyber critical infrastructure assets
- Summarize the agency's capability to respond to and recover from events that impair the ability to perform mission critical functions at or using federal cyber critical infrastructure assets
- Summarize the agency's ability to identify gaps in carrying out any of the activities discussed above
- Describe the agency's process for determining budget and personnel requirements for cyber critical infrastructure activities
- Describe the agency's process for ensuring independent oversight of cyber CIP programs
- Describe any corrective actions identified for cyber-related issues and if follow-on actions were taken
- Determine whether corrective actions for IT systems considered critical infrastructure were included in FISMA plans of action and milestones

19

Results: Objective 2

OMB Memorandum 04-15 cyber and related CIP planning criteria (cont.)

Identifying prioritized list of the agency's cyber-related critical infrastructure

- Include a prioritized list of the agency's cyber-related infrastructure assets.

Developing a long-term protective strategy

- Describe the agency's long-term protective strategy to protect the cyber critical infrastructure identified in the plan
- Describe performance metrics for the CIP program
- Describe the status of major initiatives that are underway or planned for addressing cyber-related deficiencies
- Describe milestones for the initiatives described and target dates for completing each milestone
- Discuss any specific management, technical, or operational challenges with regard to implementation of the plan

20

Results: Objective 2

Of the 18 plans submitted to OMB stating that the agency owned or operated cyber critical infrastructure,

- 4 agencies fully addressed all of the 19 criteria; they are the Department of Energy, the Environmental Protection Agency, the Social Security Administration, and the Department of State; and
- 14 fully addressed some criteria and only partially or did not address others. The 14 are shown in table 1, along with the number of criteria their plans fully addressed, partially addressed, or did not address at all.

21

GAO Accountability • Integrity • Reliability

Results: Objective 2

Table 1: Agencies Whose Initial Plans Fully Addressed Some Criteria and Only Partially Addressed or Did Not Address Others at All

Agency	Fully addressed[a]	Partially addressed[b]	Not addressed[c]
Agriculture	18	1	0
Commerce	15	1	3
Defense	17	0	2
Health and Human Services	8	0	11
Homeland Security	17	0	2
Interior	16	1	2
Justice	14	0	5
Labor	12	0	7
National Aeronautics and Space Administration	18	0	1
Office of Personnel Management	17	1	1
Small Business Administration	9	0	10

[a]Fully addressed – the plan specifically addressed the criterion.

[b]Partially addressed – the plan addressed some but not all parts of the criterion.

[c]Not addressed – the plan did not specifically address the criterion.

22

Results: Objective 2

Agency	Fully addressed[a]	Partially addressed[b]	Not addressed[c]
Transportation	17	0	2
Treasury	18	0	1
Veterans Affairs	10	2	7

Source: GAO analysis.

[a]Fully addressed – the plan specifically addressed the criterion.

[b]Partially addressed – the plan addressed some but not all parts of the criterion.

[c]Not addressed – the plan did not specifically address the related criterion.

23

Results: Objective 2

Specifically, while each of the 14 agencies fully addressed at least 8 or more criteria (for example, Health and Human Services plan fully addressed 8, and Agriculture's addressed nearly all, with 18), they also only partially addressed or did not address other criteria essential to effectively planning for the protection of cyber assets. For example, 8 agencies did not address the requirement to describe the agency's long-term strategy to protect its cyber critical infrastructure. These agencies were the Departments of Commerce, Health and Human Services, the Interior, Justice, Labor, and Veterans Affairs, the Office of Personnel Management, and the Small Business Administration. Having such a strategy is important because it establishes, among other things, agencywide direction on improving the state of cyber protection, what that future state is to be, and how and when the agency is to get there. Without such a strategy, there is increased risk that critical cyber assets may be left unprotected and thus vulnerable to threats such as unauthorized access, theft, or sabotage.

24

Results: Objective 2

In addition, the requirement to provide a summary of the agency's mission-supporting cyber assets and their locations was only partially addressed by 2 agencies (the Department of the Interior and the Office of Personnel Management) and not addressed at all by 4 (the Departments of Homeland Security, Health and Human Services, and Transportation and the National Aeronautics and Space Administration). The 2 that only partially addressed the requirement did so in that they provided the locations of their assets but did not identify the specific assets at the locations. Fully addressing this requirement is important because locating cyber assets is a key step in identifying and prioritizing assets to be protected. Without it, there is risk that not all critical cyber assets will be considered and incorporated into agency protective plans and thus will be left vulnerable to attack.

Further, 6 agencies did not address the requirement to summarize whether they had the ability to identify gaps in recovering from mission-impairing events. The 6 agencies were the Departments of Commerce, Health and Human Services, Labor, and Veterans Affairs, the National Aeronautics and Space Administration, and the Small Business Administration. Having and documenting this capability is important because it serves as an indicator that agencies are proactively identifying and managing potential risks to their cyber and other assets that could impact agency operations. Without this, there is a risk that agencies are not prepared to recover cyber assets in the event of an attack.

25

Results: Objective 2

Moreover, 5 agencies—the Departments of Health and Human Services, Justice, Labor, and Veterans Affairs, and the Small Business Administration—did not identify whether they had metrics to measure how well their cyber CIP program was performing as called for by the criteria. Having such metrics is important because they provide a basis for improving program activities and reallocating resources as needed. Without them, agencies face the risk that cyber CIP program deficiencies may not be identified and addressed, leaving cyber assets vulnerable to attack.

Furthermore, 4 agencies—the Departments of Homeland Security, Health and Human Services, Transportation, and Veterans Affairs—did not address the requirement to provide a prioritized list of the agency's cyber critical infrastructure assets. Having and documenting such a list is essential to identifying the critical cyber assets, determining protection priorities, and implementing protection mechanisms. Without it, agencies' cyber CIP programs may not adequately protect all critical cyber assets.

Our complete analysis of the criteria and the number of agencies that partially addressed or did not address them (as well as those requirements that were fully addressed) is in attachment 1. Our analysis of how each agency's plan compared to the 19 criteria is in attachment 2.

26

Results: Objective 2

These shortfalls in meeting OMB's cyber and related CIP planning requirements are attributable in part to OMB not making these plans a priority and managing them as such. Specifically, officials from OMB's Office of E-Government and Information Technology stated that when the agencies' submitted their initial plans, the office reviewed and provided feedback on the adequacy of the plans but did not follow up to verify that the agencies had revised the plans to incorporate OMB's findings or to see whether CIP planning was being implemented and institutionalized. In addition, according to the officials, when OMB issued its guidance, it did not require agencies to periodically update their plans, leaving it up to the agencies' discretion as to when and how to update the plans; consequently, the agencies in large part have not updated their plans since 2004. The officials also stated that the lack of follow up on the state of these plans, including assessing whether they had been updated, was due to their attention being focused on other competing issues. In addition, they said that, since the initial plans, they believed the agencies had engaged in other CIP-related planning efforts that largely addressed the requirement shortfalls. Our analysis below shows that the agencies did engage in subsequent planning efforts that addressed some but not all essential requirement shortfalls.

27

Results: Objective 2

Specifically, since the initial plans, the following eight agencies—whose plans did not fully meet OMB requirements—have engaged in other CIP planning efforts and related activities (e.g., developing IT security program management plans, establishing corrective action tracking systems) that addressed some but not all of their OMB requirement shortfalls:

- In its 2004 plan, the Department of Commerce did not fully address 4 cyber CIP planning requirements, including summarizing its capability to respond to and recover from events that impair performance or use of its cyber assets. However, in 2005, the department developed another CIP plan which fully addressed this criterion. Despite this, the department's 2005 plan did not fully address the 3 other criteria for which shortfalls were identified in its 2004 plan. These were
  - summarizing its ability to identify response and recovery gaps,
  - describing its process for determining budget and personnel requirements for cyber activities, and
  - describing its long-term protective strategy for protecting cyber assets.

28

Results: Objective 2

- With regard to Health and Human Services, it did not address 11 requirements in its 2004 plan, including a summary of its ability to identify response and recovery gaps, the agency's process for ensuring independent oversight over its CIP program, a prioritized list of the agency's cyber-related critical infrastructure, the agency's long-term protective strategy, a description of major initiatives for addressing cyber-related deficiencies, and milestones for these initiatives. However, in 2005 and 2008, the agency developed other plans—both entitled Secure One HHS Critical Infrastructure Protection Plan—that included these requirements, increasing the number of fully addressed requirements to 13. Consequently, the agency has yet to fully address the 6 other requirements, including describing performance metrics for the agency's CIP program and challenges to implementing the CIP plan.
- The Department of the Interior's 2004 plan did not fully address 3 requirements, including (1) providing a summary of locations and assets supporting primary functions, (2) describing the department's process to identify and track corrective actions for the cyber CIP program, and (3) describing a long-term protective strategy. Since then, the department has addressed two of these (e.g., it implemented an automated tool to track cyber security efforts and developed a long-term cyber asset protection strategy) but still has not addressed the third.

29

Results: Objective 2

- In the Department of Justice's 2004 plan, the department did not fully address 5 of OMB's requirements—namely, it did not describe
  - the agency's long term protective strategy,
  - performance metrics for the agency's CIP program,
  - the major initiatives for addressing cyber-related deficiencies,
  - milestones for these initiatives, and
  - challenges to implementation of the plan.

  Since then, the department, via other planning efforts (e.g., its IT Security Program Management Plan), has addressed all but the last requirement.
- In its 2004 plan, the National Aeronautics and Space Administration fully addressed all but the requirements to summarize (1) the locations and assets supporting primary functions and (2) the agency's ability to identify performance gaps in incident response and recovery activities. An updated addendum to the CIP plan met the first requirement. However, the second requirement remains unaddressed.

30

Results: Objective 2

- The Small Business Administration's 2004 plan did not fully address 10 requirements; however, in 2005, the agency addressed one of the missing requirements (i.e., determining whether corrective actions for IT systems considered critical infrastructure were included in FISMA plans of action and milestones) as part of other CIP planning efforts. However, these efforts did not fully address the 9 other criteria shortfalls identified in the agency's 2004 plan, such as describing the agency's ability to protect its cyber-related critical assets and its long-term protective strategy.
- Although the Department of Transportation's 2004 plan fully addressed 17 of the 19 requirements, it did not address the requirements to summarize the locations and assets that support the primary functions and include a prioritized list of the agency's cyber-related infrastructure assets. In 2008, the department developed a FISMA report that provided a summary of the location and assets supporting the primary functions; however, the requirement to provide a prioritized list of the agency's cyber-related infrastructure assets was not addressed.

31

Results: Objective 2

- In its 2004 plan, the Department of Veterans Affairs fully addressed 10 OMB requirements but did not address others such as providing
  - a description of the department's capabilities for identifying, assessing vulnerabilities for, and prioritizing its cyber CIP assets;
  - a summary of its ability to identify performance gaps in incident response and recovery activities;
  - a description of its long-term protective strategy;
  - CIP program performance metrics;
  - milestones for major cyber initiatives; and
  - a discussion of challenges to implementing the plan.

In a December 2008 update of the plan and related documentation, the department addressed 3 of the above requirements (i.e., performance metrics, milestones, and plan implementation challenges) but has yet to address the others.

32

Results: Objective 2

The above recent efforts are steps in the right direction, but until all the plans have been updated to fully address the OMB criteria, there is an increased risk that the federal government will not have effectively identified, prioritized, and protected its cyber critical assets, leaving them potentially vulnerable to deliberate efforts to destroy, incapacitate, or exploit them. This also raises questions about the usefulness of these partially-completed plans as input into the National Infrastructure Protection Plan and as a tool for initiating and institutionalizing cyber CIP planning governmentwide.

33

Conclusions

The major federal agencies' 2004 cyber CIP plans were an initial step toward the goals of (1) securing and protecting critical infrastructure and assets vital to carrying out the government's mission-critical operations and (2) implementing and institutionalizing cyber planning governmentwide. While none of the 2004 plans have since been updated, subsequent cyber CIP planning efforts by a third of the agencies have yielded additional steps toward these goals. However, continuing shortfalls in these planning efforts highlight that more remains to be done to ensure cyber CIP plans are developed in a comprehensive manner. These shortfalls are attributable in part to OMB not making these plans a priority, including not effectively overseeing agencies' efforts to make sure OMB requirements are addressed in agency plans and the plans are being implemented. Without more sustained leadership, management, and oversight in this area, there is an increased risk that federal agencies individually, and the federal government collectively, will not, among other things, effectively identify, prioritize, and protect their cyber critical assets, thus leaving them potentially vulnerable to deliberate efforts to destroy, incapacitate, or exploit them.

34

Recommendations for Executive Action

Accordingly, we recommend that the Director of the Office of Management and Budget provide leadership and oversight in directing federal cyber critical infrastructure planning efforts and make them a management priority by

- directing the agencies to expeditiously update their plans to fully address the office's cyber critical infrastructure planning requirements, and
- following up with the agencies as appropriate to make sure updated plans fully meet OMB requirements and are being effectively implemented. At a minimum, this should include having agency heads report to OMB when updated plans have been completed and that the plans fully meet OMB requirements and are being effectively implemented.

35

Agency Comments and Our Evaluation

In oral comments on a draft of this briefing, OMB officials, including the Lead Information Technology Policy Analyst from the Office of E-Government and Information Technology, agreed with our findings and first recommendation and discussed issuing a clarifying memorandum to direct agencies to update their plans. With regard to our second recommendation, these officials said that it was ultimately the responsibility of the agencies to follow up to make sure plans are effectively updated and implemented. We concur that agencies have a key role to play in updating and implementing these plans due to their knowledge of their cyber CIP environments and, therefore, know how best to secure and protect them. This notwithstanding, as previously discussed, OMB has an important role of reviewing and approving agency plans across the entire federal government to ensure that they are consistently developed, updated, and implemented. To do this effectively, OMB should periodically follow up with the agencies to assess the status and progress of cyber CIP planning efforts.

GAO
Accountability * Integrity * Reliability

Attachment 1
Overall Summary Analysis of Criteria and the 2004 Plans

The following table illustrates the number of plans that fully, partially, and did not address each criterion (organized by key topic area).

Criteria by key topic area	No. of plans that fully addressed	No. of plans that partially addressed	No. of plans that did not address
Addressing existing capabilities for protecting federal cyber critical infrastructure			
Summarize primary functions of the agency that rely on cyber critical infrastructure assets	18	0	0
Summarize the agency's management structure, including the management responsible for the security of cyber critical assets	18	0	0
Summarize locations and assets that support the primary functions	12	2	4
Describe the agency's current capabilities for identification of federally owned or operated cyber critical infrastructure assets	17	1	0
Describe the agency's current capabilities for assessments of cyber vulnerabilities and interdependencies	17	1	0
Describe the agency's current capabilities for prioritization of federal cyber assets	15	1	2
Describe the agency's current capabilities for adequately protecting cyber critical infrastructure assets	17	0	1

37

GAO Accountability • Integrity • Reliability

Attachment 1

Overall Summary Analysis of Criteria and the 2004 Plans (cont.)

Criteria by key topic area	No. of plans that fully addressed	No. of plans that partially addressed	No. of plans that did not address
Summarize the agency's capability to respond to and recover from events that impair the ability to perform mission critical functions at or using federal cyber critical infrastructure assets	17	0	1
Summarize the agency's ability to identify gaps in carrying out any of the activities discussed above	12	0	6
Describe the agency's process for determining budget and personnel requirements for cyber critical infrastructure activities	16	1	1
Describe the agency's process for ensuring independent oversight of cyber CIP programs	14	0	4
Describe any corrective actions identified for cyber-related issues and if follow-on actions were taken	13	0	5
Determine whether corrective actions for IT systems considered critical infrastructure were included in Federal Information Security Management Act (FISMA) plans of action and milestones.	14	0	4
Prioritized list of the agency's cyber-related critical infrastructure			
Include a prioritized list of the agency's cyber-related critical infrastructure	14	0	4

38

GAO
Accountability * Integrity * Reliability

Attachment 1
Overall Summary of Criteria and the 2004 Plans (cont.)

Criteria by key topic area	No. of plans that fully addressed	No. of plans that partially addressed	No. of plans that did not address
Developing a long-term protective strategy			
Describe the agency's long-term protective strategy to protect the cyber critical infrastructure identified in the plan	10	0	8
Describe performance metrics for the CIP program	13	0	5
Describe the status of major initiatives that are underway or planned for addressing cyber-related deficiencies	16	0	2
Describe milestones for the initiatives described and target dates for completing each milestone	15	0	3
Discuss any specific management, technical, or operational challenges with regard to implementation of the plan.	13	0	5

Source: GAO analysis of agency plans.

GAO
Accountability • Integrity • Reliability

Attachment 2

Criteria Met by 2004 Cyber CIP Plans of Major Federal Agencies

Agriculture–Justice

Criteria (by key topic area)	USDA	DOC	DOD	DHS	DOE	EPA	HHS	DOI	DOJ
Addressing existing capabilities for protecting federal cyber critical infrastructure									
Summarize primary functions of the agency that rely on cyber critical infrastructure assets	●	●	●	●	●	●	●	●	●
Summarize the agency's management structure, including the management responsible for the security of cyber critical assets	●	●	●	●	●	●	●	●	●
Summarize the locations and assets that support the primary functions	●	●	●	○	●	●	○	◐[a]	●
Describe the agency's current capabilities for identification of federally owned or operated cyber critical infrastructure assets	●	●	●	●	●	●	●	●	●
Describe the agency's current capabilities for assessments of cyber vulnerabilities and interdependencies	●	●	●	●	●	●	●	●	●
Describe the agency's current capabilities for prioritization of federal cyber assets	◐[b]	●	●	●	●	●	●	●	●

Legend: ●=fully addressed ◐=partially addressed ○=not addressed

Note: Agency abbreviations as follows: Agriculture (USDA), Defense (DOD), Homeland Security (DHS), Energy (DOE), Environmental Protection Agency (EPA), Health and Human Services (HHS), Interior (DOI), and Justice (DOJ).

[a]The Department of the Interior's plan discussed the function and locations but did not identify the assets.

[b]The Department of Agriculture's plan described a process but did not address whether the department had prioritized its cyber assets.

40

GAO Accountability • Integrity • Reliability

Attachment 2

Criteria Met by 2004 Cyber CIP Plans of Major Federal Agencies

Agriculture–Justice (cont.)

Criteria (by key topic area)	USDA	DOC	DOD	DHS	DOE	EPA	HHS	DOI	DOJ
Describe the agency's current capabilities for adequately protecting cyber critical infrastructure assets	●	●	●	●	●	●	●	●	●
Summarize the agency's capability to respond to and recover from events that impair the ability to perform mission critical functions at or using federal cyber critical infrastructure assets	●	○	●	●	●	●	●	●	●
Summarize the agency's ability to identify gaps in carrying out any of the activities discussed above	●	○	●	●	●	●	○	●	●
Describe the agency's process for determining budget and personnel requirements for cyber critical infrastructure activities	●	◐[c]	●	●	●	●	●	●	●
Describe the agency's process for ensuring independent oversight of cyber CIP programs	●	●	○	●	●	●	○	●	●
Describe any corrective actions identified for cyber-related issues and if follow-on actions were taken	●	●	●	●	●	●	○	○	●
Determine whether corrective actions for IT systems considered critical infrastructure were included in Federal Information Security Management Act (FISMA) plans of action and milestones.	●	●	○	●	●	●	○	●	●

Legend: ●=fully addressed ◐=partially addressed ○=not addressed

Note: Agency abbreviations as follows: Agriculture (USDA), Defense (DOD), Homeland Security (DHS), Energy (DOE), Environmental Protection Agency (EPA), Health and Human Services (HHS), Interior (DOI), and Justice (DOJ).

[c]The Department of Commerce's plan identified special funding but did not provide an overall process for determining resources.

41

GAO
Accountability • Integrity • Reliability

Attachment 2
Criteria Met by 2004 Cyber CIP Plans of Major Federal Agencies

Agriculture–Justice (cont.)

Criteria (by key topic area)	USDA	DOC	DOD	DHS	DOE	EPA	HHS	DOI	DOJ
Prioritized list of agency-owned or operated critical infrastructure									
Include a prioritized list of the agency's cyber-related critical infrastructure	●	●	●	○	●	●	○	●	●
Long-term protective strategy									
Describe the agency's long-term protective strategy to protect the cyber critical infrastructure identified in the plan	●	○	●	●	●	●	○	○	○
Describe the performance metrics for the CIP program	●	●	●	●	●	●	○	●	○
Describe the status of major initiatives that are underway or planned for addressing cyber-related deficiencies	●	●	●	●	●	●	○	●	○
Describe the milestones for the initiatives described and target dates for completing each milestone	●	●	●	●	●	●	○	●	○
Discuss any specific management, technical, or operational challenges with regard to implementation of the plan.	●	●	●	●	●	●	○	●	○

Legend: ●=fully addressed ◐=partially addressed ○=not addressed

Note: Agency abbreviations as follows: Agriculture (USDA), Defense (DOD), Homeland Security (DHS), Energy (DOE), Environmental Protection Agency (EPA), Health and Human Services (HHS), Interior (DOI), and Justice (DOJ).

GAO Accountability • Integrity • Reliability

Attachment 2

Criteria Met by 2004 Cyber CIP Plans of Major Federal Agencies

Labor–Veterans Affairs

Criteria (by key topic area)	Labor	NASA	OPM	SBA	SSA	State	DOT	Treas.	VA
Addressing existing capabilities for protecting federal cyber critical infrastructure									
Summarize primary functions of the agency that rely on cyber critical infrastructure assets	●	●	●	●	●	●	●	●	●
Summarize the agency's management structure, including the management responsible for the security of cyber critical assets	●	●	●	●	●	●	●	●	●
Summarize the locations and assets that support the primary functions	●	○	◐[d]	●	●	●	○	●	●
Describe the agency's current capabilities for identification of federally owned or operated cyber critical infrastructure assets	●	●	●	●	●	●	●	●	◐[e]
Describe the agency's current capabilities for assessments of cyber vulnerabilities and interdependencies	●	●	●	●	●	●	●	●	◐[f]

Legend: ●=fully addressed ◐=partially addressed ○=not addressed

Note: Agency abbreviations are as follows: National Aeronautics and Space Administration (NASA), Office of Personnel Management (OPM), Small Business Administration (SBA), Social Security Administration (SSA), Transportation (DOT), and Veterans Affairs (VA).

[d]The Office of Personnel Management's plan summarized the locations but did not identify the specific assets.

[e]The Department of Veterans Affairs' plan described the department's capability to identify assets but did not state how the process included cyber assets.

[f]The Department of Veterans Affairs' plan described departmental capability to perform vulnerability assessments but did not specify how the process included cyber assets.

43

GAO
Accountability • Integrity • Reliability

Attachment 2

Criteria Met by 2004 Cyber CIP Plans of Major Federal Agencies

Labor–Veterans Affairs (cont.)

Criteria (by key topic area)	Labor	NASA	OPM	SBA	SSA	State	DOT	Treas.	VA
Describe the agency's current capabilities for prioritization of federal cyber assets	●	●	●	○	●	●	●	●	○
Describe the agency's current capabilities for adequately protecting cyber critical infrastructure assets	●	●	●	○	●	●	●	●	●
Summarize the capability to respond to and recover from events that impair the ability to perform mission critical functions at or using federal cyber critical infrastructure assets	●	●	●	●	●	●	●	●	●
Summarize the ability to identify gaps in carrying out any of the activities discussed above	○	○	●	○	●	●	●	●	○
Describe the agency's process for determining budget and personnel requirements for cyber critical infrastructure activities	●	●	●	○	●	●	●	●	●
Describe the agency's process for ensuring independent oversight of cyber CIP programs	○	●	●	○	●	●	●	●	●
Describe any corrective actions identified for cyber-related issues and if follow-on actions were taken	○	●	●	○	●	●	●	○	●

Legend: ●=fully addressed ◐=partially addressed ○=not addressed

Note: Agency abbreviations are as follows: National Aeronautics and Space Administration (NASA), Office of Personnel Management (OPM), Small Business Administration (SBA), Social Security Administration (SSA), Transportation (DOT), and Veterans Affairs (VA).

GAO
Accountability • Integrity • Reliability

Attachment 2

Criteria Met by 2004 Cyber CIP Plans of Major Federal Agencies

Labor–Veterans Affairs (cont.)

Criteria (by key topic area)	Labor	NASA	OPM	SBA	SSA	State	DOT	Treas.	VA
Determine whether corrective actions for IT systems considered critical infrastructure were included in Federal Information Security Management Act (FISMA) plans of action and milestones.	○	●	●	○	●	●	●	●	●
Prioritized list of agency-owned or operated critical infrastructure									
Include a prioritized list of agency cyber-related critical infrastructure	●	●	●	●	●	●	○	●	○
Long-term protective strategy									
Describe the agency's long-term protective strategy to protect the cyber critical infrastructure identified in the plan	○	●	○	○	●	●	●	●	○
Describe the performance metrics for the CIP program	○	●	●	○	●	●	●	●	○
Describe the status of major initiatives that are underway or planned for addressing cyber-related deficiencies	●	●	●	●	●	●	●	●	●
Describe the milestones for the initiatives described and target dates for completing each milestone	●	●	●	●	●	●	●	●	○
Discuss any specific management, technical, or operational challenges with regard to implementation of the plan.	○	●	●	○	●	●	●	●	○

Legend: ●=fully addressed ◐=partially addressed ○=not addressed

Note: Agency abbreviations are as follows: National Aeronautics and Space Administration (NASA), Office of Personnel Management (OPM), Small Business Administration (SBA), Social Security Administration (SSA), Transportation (DOT), and Veterans Affairs (VA).

Source: GAO analysis of agency plans.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, key contributions were made to this report by Gary N. Mountjoy, Assistant Director; Nabajyoti Barkakati; Scott F. Borre; Neil J. Doherty; Michael W. Gilmore; Barbarol J. James; Kenneth A. Johnson; Kush K. Malhotra; and Lee A. McCracken.

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