United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2010

CYBERSPACE POLICY

Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed

GAO-11-24

October 2010

CYBERSPACE POLICY

Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-24, a report to congressional requesters

Why GAO Did This Study

To address pervasive computer-based (cyber) attacks against the United States that posed potentially devastating impacts to systems and operations, the federal government has developed policies and strategies intended to combat these threats. A recent key development was in February 2009, when President Obama initiated a review of the government's overall strategy and supporting activities with the aim of assessing U.S. policies and structures for cybersecurity. The resulting policy review report—issued by the President in May 2009—provided 24 near- and mid-term recommendations to address these threats.

GAO was asked to assess the implementation status of the 24 recommendations. In doing so, GAO, among other things, analyzed the policy review report and assessed agency documentation and interviewed agency officials.

What GAO Recommends

GAO recommends that the national Cybersecurity Coordinator designates roles and responsibilities and develops milestones and plans for the recommendations that lacked these key planning elements. The Cybersecurity Coordinator's office provided no comments on the conclusions and recommendations in this report; the office did cite recent progress being made on cybersecurity research and development and education that is consistent with GAO's report.

View GAO-11-24 or key components.
For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Of the 24 recommendations in the President's May 2009 cyber policy review report, 2 have been fully implemented, and 22 have been partially implemented. The two fully implemented recommendations involve appointing within the National Security Council a cybersecurity policy official (Special Assistant to the President and Cybersecurity Coordinator) responsible for coordinating the nation's cybersecurity policies and activities, and a privacy and civil liberties official. Examples of partially implemented recommendations include:

- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties, leveraging privacy-enhancing technologies for the nation: In June 2010, the administration released a draft strategy (entitled National Strategy for Trusted Identities in Cyberspace) that seeks to increase trust associated with the identities of individuals, organizations, services, and devices involved in financial and other types of online transactions, as well as address privacy and civil liberty issues associated with identity management. It plans to finalize the strategy in October 2010.
- Develop a framework for research and development strategies: The administration's Office of Science and Technology Policy (which is within the Executive Office of the President) has efforts under way to develop a framework for research and development strategies, which as currently envisioned includes three key cybersecurity research and development themes, but is not expected to be finalized until 2011.

Officials from key agencies involved in these cybersecurity efforts, (e.g., the Departments of Defense and Homeland Security and the Office of Management and Budget) attribute the partial implementation status of the 22 recommendations in part to the fact that agencies are moving slowly because they have not been assigned roles and responsibilities with regard to recommendation implementation. Specifically, although the policy review report calls for the cybersecurity policy official to assign roles and responsibilities, agency officials stated they have yet to receive this tasking and attribute this to the fact that the cybersecurity policy official position was vacant for 7 months. In addition, officials stated that several mid-term recommendations are broad in nature, and agencies state they will require action over multiple years before they are fully implemented. This notwithstanding, federal agencies reported they have efforts planned or under way that are aimed toward implementing the 22 partially implemented recommendations. While these efforts appear to be steps forward, agencies were largely not able to provide milestones and plans that showed when and how implementation of the recommendations was to occur. Specifically, 16 of the 22 near- and mid-term recommendations did not have milestones and plans for implementation. Consequently, until roles and responsibilities are made clear and the schedule and planning shortfalls identified above are adequately addressed, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.

Contents

Abbreviations

CNCI	Comprehensive National Cybersecurity Initiative
DHS	Department of Homeland Security
DOD	Department of Defense
ICI-IPC	Information and Communication Infrastructure-Interagency Policy Committee
OMB	Office of Management and Budget
NIST	National Institute of Standards and Technology
NSC	National Security Council
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 6, 2010

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

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

To address pervasive and sustained computer-based (cyber) attacks against the United States that posed potentially devastating impacts to systems and operations and the critical infrastructures that they support,[1] the federal government developed policies and strategies intended to combat these threats. For example, in 2003, President Bush issued a national strategy and related policy directives aimed at improving cybersecurity nationwide, including both government systems and those cyber critical infrastructures owned and operated by the private sector. In addition, in 2008, the Bush Administration began to implement a series of initiatives, referred to as the Comprehensive National Cybersecurity Initiative (CNCI), aimed primarily at improving cybersecurity within the federal government.

More recently, in February 2009, President Obama initiated a review of the government's overall cybersecurity strategy and supporting activities with the aim of assessing U.S. policies and structures for cybersecurity. The resulting May 2009 report provided 24 near- and mid-term

[1]Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; public health and health care; transportation systems; and water.

recommendations, also referred to as action items, to address threats and improve the current U.S. approach to cybersecurity.

The report also called for appointing a national cybersecurity policy official within the National Security Council (NSC) to coordinate the nation's cybersecurity policies and activities. In December 2009, the President appointed a Special Assistant to the President and Cybersecurity Coordinator (herein referred to as the Cybersecurity Coordinator) to fulfill this role.

In response to your request to review the May 2009 report, our objective was to assess the implementation status of the 24 near- and mid-term recommendations. On August 2 and 5, 2010, we provided briefings on the results of our review to staff of the Committee on Homeland Security, and Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, House Committee on Homeland Security. Prior to those briefings, we provided a draft of the briefing presentation slides (that we intended to use to brief the staff) to the national Cybersecurity Coordinator for review and comment and incorporated (July 23, 2010) comments provided by the Director of Cybersecurity within the national Cybersecurity Coordinator's office. This report summarizes and transmits (1) the final presentation slides we used to brief the staff and (2) recommendations to the Cybersecurity Coordinator 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 November 2009 to October 2010, 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.

While 2 Recommendations Have Been Fully Implemented, 22 Are in Process

Of the 24 recommendations in the President's May 2009 cyber policy review report, 2 have been fully implemented, and 22 have been partially implemented. The two fully implemented recommendations involve appointing within the NSC

- a cybersecurity policy official responsible for coordinating the nation's cybersecurity policies and activities, and
- a privacy and civil liberties official.

Examples of partially implemented recommendations include

- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties, leveraging privacy-enhancing technologies for the nation: In June 2010, the administration released a draft strategy (entitled National Strategy for Trusted Identities in Cyberspace) that seeks to increase trust associated with the identities of individuals, organizations, services, and devices involved in financial and other types of online transactions, as well as address privacy and civil liberty issues associated with identity management. The administration plans to finalize the strategy in October 2010.
- Develop a framework for research and development strategies: The administration's Office of Science and Technology Policy (which is within the Executive Office of the President) has efforts under way to develop a framework for research and development strategies, which as currently envisioned includes three key cybersecurity research and development themes but is not expected to be finalized until 2011.

Officials from key agencies involved in these cybersecurity efforts, (e.g., Department of Homeland Security, the Department of Defense, and the Office of Management and Budget) attribute the partial implementation status of the 22 recommendations to the following:

- Agencies are moving slowly because they have not been assigned roles and responsibilities with regard to recommendation implementation. Specifically, although the policy review report calls for the Cybersecurity Coordinator to assign roles and responsibilities, agency officials stated they have yet to receive this tasking and attribute this to the fact that the Cybersecurity Coordinator position was vacant for 7 months.

- Several mid-term recommendations are broad in nature, and agencies state they will require action over multiple years before they are fully implemented. For example, agencies officials told us the mid-term recommendation to expand sharing of information about network incidents and vulnerabilities with key allies is very broad, will require additional guidance in order to be fully implemented, and thus could take a number of years to complete.

This notwithstanding, federal agencies reported they have efforts planned or under way that are aimed toward implementing the 22 partially implemented recommendations. While these appear to be steps forward, agencies were largely not able to provide milestones and plans that showed when and how implementation of the recommendations was to occur. Specifically, 16 of the 22 near- and mid-term recommendations did not have milestones and plans for implementation. Our extensive research and experience at federal agencies have shown that, without clearly and explicitly assigned roles and responsibilities and documented plans, agencies increase the risk that implementing such actions will not fully succeed. Consequently, until roles and responsibilities are made clear, and the schedule and planning shortfalls identified above are adequately addressed, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.

Conclusions

Although it has been over a year since the Executive Branch issued the results of its 2009 cyberspace policy review, agencies have yet to be assigned roles and responsibilities to implement a large majority of the near- and mid-term recommendations specified in the review. This notwithstanding, federal agencies appear to be making progress toward implementing the recommendations but lack milestones, plans, and measures that are essential to ensuring successful recommendation implementation. The above shortcomings are attributable in part to the Cybersecurity Coordinator position being vacant for a critical period of time immediately following issuance of the recommendations. Consequently, going forward, it is essential that the Cybersecurity Coordinator address these shortfalls. Until then, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.

Recommendations for Executive Action

We recommend the Special Assistant to the President and Cybersecurity Coordinator, as part of implementing the 22 outstanding recommendations,

- designate roles and responsibilities for each recommendation, including which agencies are leading and supporting the effort; and
- develop milestones and plans, including measures to show agency implementation progress and performance, for the 16 recommendations identified in attachment I that lacked these key planning elements.

Agency Comments and Our Evaluation

In an e-mail transmitting comments on a draft of this report, the Director for Cybersecurity within the office of the national Cybersecurity Coordinator provided no additional comments on our conclusions and recommendations beyond those he provided in July 2010 on the draft briefing slides (see appendix I, page 39). The Director did provide additional comments on progress he cited was being made on cyberspace policy review recommendations in the areas of cybersecurity research and development and education. First, with regard to the policy review recommendation to develop a framework for research and development strategies, the Director stated that a game-changing research and development strategy was completed in May 2010. While we acknowledge this reported progress, we also point out (as we did in our briefing slides) that the themes of the strategy/framework do not incorporate all priorities that should be included in a comprehensive national cybersecurity research and development agenda that is to serve as guidance for prioritizing federal cybersecurity research and development activities.

Second, with regard to the recommendation to initiate a public awareness and education campaign to promote cybersecurity, the Director commented that a public kickoff for the National Initiative for Cybersecurity Education, led by the National Institute for Standards and Technology, was held in August 2010. While we acknowledge this progress and agree it is an important step toward initiating a public awareness and education campaign, we also point out (as we did in our briefing slides) that the Cybersecurity Coordinator has stated that milestones and plans, among other things, have yet to be developed for completing this recommendation.

We are sending copies of this report to the appropriate congressional committees; the Special Assistant to the President and Cybersecurity Coordinator; the Secretaries of Commerce, Defense, and Homeland Security; the Directors of the National Science Foundation and the Office of Management and Budget; and other interested parties. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff members have questions on matters discussed in this report, please contact David 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 major 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

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Needed

Briefing for Staff Members of the

House Committee on Homeland Security and

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology,

House Committee on Homeland Security

August 2, 2010

Briefing Overview

Introduction

Objective, Scope, and Methodology

Results in Brief

Background

Results

Conclusions

Recommendations for Executive Action

Agency Comments and Our Evaluation

Attachment I

2

Introduction

To address pervasive and sustained computer-based (cyber) attacks against the United States that posed potentially devastating impacts to systems and operations and the critical infrastructures that they support,[1] the federal government has developed policies and strategies intended to combat these threats. For example, in 2003 President Bush issued a national strategy and related policy directives aimed at improving cybersecurity nationwide, including both government systems and those cyber critical infrastructures owned and operated by the private sector. In addition, in 2008, the Bush Administration began to implement a series of initiatives, referred to as the Comprehensive National Cybersecurity Initiative (CNCI), aimed primarily at improving cybersecurity within the federal government.

[1]Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; public health and health care; transportation systems; and water.

3

Introduction

More recently, in February 2009, President Obama initiated a review of the government's overall cybersecurity strategy and supporting activities with the aim of assessing U.S. policies and structures for cybersecurity. The resulting report provided 24 near- and mid-term recommendations, also referred to as action items, to address these threats and implement changes to the current U.S. approach to cybersecurity. Examples of recommendations include:

- prepare a cybersecurity incident response plan;
- develop a framework for research and development strategies;
- expand sharing of information about network incidents and vulnerabilities with key allies; and
- expand support for key education programs and research and development.

The report also called for appointing a national cybersecurity policy official within the National Security Council (NSC) to coordinate the Nation's cybersecurity policies and activities. In response, the President appointed a Special Assistant to the President and Cybersecurity Coordinator in December 2009 (herein referred to as the Cybersecurity Coordinator) to fulfill this role. The report did not provide a specific timeline for when the near- and mid-term recommendations were to be implemented.

4

Objective, Scope, and Methodology

As agreed, our objective was to assess the implementation status of the 24 near- and mid-term recommendations.

To address the objective, we analyzed the cyberspace policy review report[2] and supporting documents and interviewed administration and agency officials to determine the extent to which roles and responsibilities had been assigned for implementation of the near- and mid-term recommendations. This included analyzing agency documentation and interviewing agency officials to determine the status of and extent to which actions to address the 24 specific near- and mid-term recommendations had been implemented. We also analyzed ongoing cybersecurity initiatives that were underway prior to the cyberspace policy review that correspond to the recommendations and interviewed officials from agencies—such as the Department of Defense (DOD), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB)—that are involved in these efforts.

[2] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., May 29, 2009).

5

Objective, Scope, and Methodology

In analyzing the status of the near- and mid-term recommendations, we categorized the extent to which the recommendations had been implemented using the following criteria:

- *fully implemented:* if all aspects of the near- or mid-term recommendation were developed and instituted
- *partially implemented:* if not fully implemented but at least one aspect of the near- or mid-term recommendation is being developed or instituted
- *not implemented:* if none of the aspects of the near- or mid-term recommendation is being developed or instituted.

We conducted this performance audit from November 2009 through July 2010, 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

Of the 24 recommendations in the President's May 2009 cyber policy review report, 2 have been fully implemented and 22 have been partially implemented. The two fully implemented recommendations involve appointing within the NSC

- a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities and
- a privacy and civil liberties official.

Examples of partially implemented recommendations include

- Prepare a cybersecurity incident response plan: In March 2010, DHS issued a draft cybersecurity incident response plan—called the National Cyber Incident Response Plan. However, the plan is not to be finalized until late summer 2010.
- Develop a framework for research and development strategies: The Administration's Office of Science and Technology Policy (which is within the Executive Office of the President) has efforts underway to develop a framework for research and development strategies, which as currently envisioned includes three key cybersecurity research and development themes, but is not expected to be finalized until 2011.

Results in Brief

Officials from key agencies involved in these cybersecurity efforts, (e.g. DHS, DOD, and OMB) attribute the partial implementation status of the 22 recommendations to the following:

- Agencies are moving slowly because they have not been assigned roles and responsibilities with regard to recommendation implementation. Specifically, although the policy review report calls for the Cybersecurity Coordinator to assign roles and responsibilities, agency officials stated they have yet to receive this tasking and attribute this to the fact that the Cybersecurity Coordinator position was vacant for 7 months.
- Several mid-term recommendations are broad in nature, and agencies state they will require action over multiple years before they are fully implemented. For example, agencies officials told us the mid-term recommendation to expand sharing of information about network incidents and vulnerabilities with key allies is very broad, will require additional guidance in order to be fully implemented, and thus could take a number of years to complete.

8

Results in Brief

Despite these factors, federal agencies reported they have efforts planned or underway that are aimed toward implementing the 22 partially implemented recommendations. While these appear to be steps forward, agencies were largely not able to provide milestones and plans that showed when and how implementation of the recommendations was to occur. Specifically, 16 of the 22 near- and mid-term recommendations did not have milestones and plans for implementation. Our extensive research and experience at federal agencies have shown that without clearly and explicitly assigned roles and responsibilities and documented plans, agencies increase the risk that implementing such actions will not fully succeed. Consequently, until roles and responsibilities are made clear and the schedule and planning shortfalls identified above are adequately addressed, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.

Accordingly, we are making recommendations to the Cybersecurity Coordinator to, among other things, assign clear roles and responsibilities for the 22 partially implemented near- and mid-term recommendations and develop milestones and plans for the 16 recommendations where these key activities have not been completed.

9

Results in Brief

In oral comments on a draft of this briefing, the Director for Cybersecurity within the office of the national Cybersecurity Coordinator generally concurred with our findings but took exception with our conclusions and recommendations. This official said he was in general agreement with the findings as they relate to the state of progress being made. However, regarding our conclusions, the Director commented that he read the report to have a general implication and conclusion that progress is not being made. This official stated that contrary to this implication and conclusion, important progress is being made on all fronts. We agree that progress is being made and have stated this point throughout the briefing, including the conclusions section.

With regard to our recommendations, the Director disagreed with the recommendation on assigning roles and responsibilities, noting that many policy review recommendations require contributions from multiple agency participants and those efforts are being coordinated through an interagency policy process within the Executive Office of the President. We reiterate the evidence in our briefing that agencies participating in this process said they had not been assigned roles and responsibilities with respect to recommendation implementation.

The Director also provided technical comments which we incorporated where appropriate.

Background

To address growing concerns about cyber attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations, the federal government has developed national policies and strategies aimed at combating such cyber threats. Specifically, President Bush issued the 2003 *National Strategy to Secure Cyberspace*[3] and related policy directives, such as Homeland Security Presidential Directive 7,[4] that specify key elements of how the nation is to secure key computer-based systems, including both government systems and those that support critical infrastructures owned and operated by the private sector.

In addition, in January 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23,[5] establishing CNCI, a set of projects with the objective of safeguarding federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats.

[3]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).
[4]The White House, Homeland Security Presidential Directive 7 (Washington, D.C.: Dec. 17, 2003).
[5]The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

Background

CNCI includes defensive, offensive, education, research and development, and counterintelligence efforts outlined in 12 initiatives, which include

- managing the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections;
- coordinating and redirecting research and development efforts;
- connecting current cyber operation centers to enhance situational awareness;
- expanding cyber education;
- defining and developing enduring leap-ahead technology, strategies, and programs; and
- developing a multi-pronged approach for global supply chain risk management.

12

Background

More recently, President Obama (in February 2009) initiated an extensive review of U.S. cybersecurity strategy and supporting activities with the aim of assessing U.S. policies and structures for cybersecurity. Specifically, the review assessed the missions and activities associated with the nation's information and communication infrastructure. The review resulted in a May 2009 report that included 10 near-term and 14 mid-term recommendations—without specific timelines for when they were to be implemented—aimed at helping the United States achieve a more reliable, resilient, and trustworthy digital infrastructure.

The following slides detail the 10 near-term and 14 mid-term recommendations.

13

Background
Near-term Recommendations

The 10 near-term recommendations are:

- Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate,[6] under the direction of the cybersecurity policy official dual-hatted to the NSC and the National Economic Council,[7] to coordinate interagency development of cybersecurity-related strategy and policy.
- Update the 2003 *National Strategy to Secure Cyberspace* to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
- Designate cybersecurity as one of the President's key management priorities and establish performance metrics.

[6]The National Security Council is the President's principal forum for considering national security and foreign policy matters with senior national security advisors and cabinet officials. The Council's function is to advise and assist the President on national security and foreign policies and coordinate these policies among various government agencies.
[7]The National Economic Council advises the President on U.S. and global economic policy. The Council has four principal functions: to coordinate policy-making for domestic and international economic issues, to coordinate economic policy advice for the President, to ensure that policy decisions and programs are consistent with the President's economic goals, and to monitor implementation of the President's economic policy agenda.

14

Background

Near-term Recommendations

- Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
- Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government.
- Initiate a national public awareness and education campaign to promote cybersecurity.
- Develop U.S. government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
- Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.

15

Background

Near-term Recommendations

- In collaboration with other Executive Office of the President entities, develop a framework for research and development strategies that focuses on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

16

Background
Mid-term Recommendations

The 14 mid-term recommendations are:

- Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
- Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
- Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
- Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the federal government.
- Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
- Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of research and development.

17

Background
Mid-term Recommendations

- Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
- Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
- Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
- Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
- Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
- Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.

18

Background
Mid-term Recommendations

- Implement, for high-value activities (e.g., the Smart Grid[8]), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
- Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

[8] Government and industry efforts to develop a "Smart Grid" are intended to modernize the aging U.S. electrical power transmission and distribution system, which uses technologies and strategies that are several decades old and include limited use of digital communication and control technologies. The Smart Grid would use advanced sensing, communication, and control technologies to generate and distribute electricity more effectively, economically, and securely.

19

Background

Role of the Cybersecurity Coordinator

As specified in the report, the Cybersecurity Coordinator is to have responsibility for cybersecurity policy and strategy and is to report to the NSC head and coordinate with the head of the National Economic Council. This official is also to chair the Information and Communication Infrastructure-Interagency Policy Committee (ICI-IPC), which is the primary policy coordination body within the Executive Office of the President responsible for directing and overseeing issues related to achieving a reliable global information and communications infrastructure. The report also states that the official should work with departments and agencies to recommend coherent unified policy guidance where necessary in order to clarify authorities, roles, and responsibilities for cybersecurity-related activities across the federal government.

20

Results

While 2 Recommendations Have Been Fully Implemented, 22 Are in Process

Of the 24 recommendations in the review, 2 have been fully implemented and 22 recommendations have been partially implemented. Specifically, 2 of the 10 near-term recommendations have been implemented; the remaining 8 near-term and all 14 mid-term recommendations have been partially implemented. The following table specifies the implementation status of the 10 near-term and 14 mid-term recommendations.

GAO
Accountability * Integrity * Reliability

Results
Near-term Recommendations

Recommendation	Fully Implemented	Partially Implemented
Appoint a cybersecurity policy official.	X	
Prepare for approval of an updated national strategy.		X
Designate cybersecurity as one of the President's key management priorities and establish performance metrics.		X
Designate a privacy and civil liberties official to NSC.	X	
Formulate policy guidance to clarify federal government roles.		X
Initiate a national public awareness and education campaign to promote cybersecurity.		X
Develop government positions for an international policy framework.		X
Prepare a cybersecurity incident response plan.		X
Develop a framework for research and development strategies.		X
Build a cybersecurity-based identity management vision and strategy that address privacy and civil liberties.		X

22

GAO
Accountability * Integrity * Reliability

Results
Mid-term Recommendations

Recommendation	Fully Implemented	Partially Implemented
Improve process for resolution of interagency disagreements of law and policy.		X
Use the OMB assessment framework to ensure agencies use performance-based budgeting.		X
Expand support for key education programs and research and development.		X
Develop a strategy to expand and train the workforce.		X
Determine the most efficient mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.		X
Develop a set of threat scenarios and metrics.		X
Develop a process between the government and private sector for preventing, detecting, and responding to cyber incidents.		X
Develop mechanisms for information sharing.		X
Develop solutions for emergency communications during a crisis.		X
Expand sharing of information about network incidents and vulnerabilities.		X
Encourage collaboration between academic and industrial laboratories.		X
Define goals for national and international standards bodies.		X
Implement an opt-in array of interoperable identity management systems for high-value activities.		X
Refine government procurement strategies.		X
Total	**2**	**22**

23

Results

As shown in the table, the two near-term recommendations that have been fully implemented involve appointing

- A cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities. In December 2009, the President appointed a Cybersecurity Coordinator; whose position is located within the NSC. More specifically, the position is located within a council directorate that oversees cybersecurity activities. The Cybersecurity Coordinator also is to serve as the chair of the ICI-IPC and coordinate cybersecurity activities with the National Economic Council.
- A privacy and civil liberties official. In late 2009, a civil liberties and privacy official was appointed to serve in the NSC cybersecurity directorate.

24

Results

Examples of the remaining 22 recommendations (8 near-term and 14 mid-term) that have been partially implemented include:

- Prepare a cybersecurity incident response plan: In March 2010, DHS issued a draft cybersecurity incident response plan—called the National Cyber Incident Response Plan. This plan is part of DHS's National Response Framework, which provides a unified national response to disasters and emergences, including cybersecurity incidents. However, the draft plan is not to be finalized until late summer 2010. DHS does intend to test the plan (as part of a cyber incident exercise) in September 2010.

25

Results

- Develop a framework for research and development strategies: According to officials within the Office of Science and Technology Policy, the office has recently begun developing such a framework. As currently envisioned, the framework includes three key cybersecurity research and development themes: supporting security policies and security services for different types of cyber space interactions; deploying systems that are both diverse and changing; and developing cybersecurity incentives to create foundations for cybersecurity markets and establish meaningful metrics. However, the framework is not expected to be finalized until 2011, and we recently reported[9] that the themes of the framework do not incorporate all priorities that should be included in a comprehensive national cybersecurity research and development agenda that is to serve as guidance for prioritizing federal cybersecurity research and development activities.

[9]GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development,* GAO-10-466, (Washington, D.C: June 3, 2010).

26

Results

- Build a cybersecurity-based identity management strategy that addresses privacy and civil liberties: In July 2009, the Acting White House Cybersecurity Policy Advisor stated that work had begun on a framework to set priorities in the area of identity management. Specifically, NIST and other agencies are working with an ICI-IPC subcommittee (the Architecture, Research and Development Subcommittee of the Interagency Policy Committee) to develop an identity management strategy. More recently, in June 2010, the Administration released a draft of this strategy (entitled National Strategy for Trusted Identities in Cyberspace), that seeks to increase trust associated with the identities of individuals, organizations, services, and devices involved in financial and other types of online transactions. In addition, a stated aim of the draft strategy is to address privacy and civil liberty issues associated with identity management. However, the Administration does not plan to finalize the strategy until October 2010.

Our analysis of all of the 22 partially implemented recommendations (8 near-term and 14 mid-term) is provided in attachment I.

27

Results

Officials from the agencies (e.g. DOD, DHS, and OMB) involved in key planned and ongoing cyber activities attributed the partial implementation status of the 22 (8 near-term and 14 mid-term) recommendations to

- Agencies are moving slowly since they have not been assigned roles and responsibilities with regard to recommendation implementation. Specifically, although the policy review calls for the Cybersecurity Coordinator to assign roles and responsibilities, agency officials consistently stated they have yet to receive this tasking and attribute the inaction to the fact that the Cybersecurity Coordinator position was vacant for approximately 7 months.
- Several mid-term recommendations are broad in nature, and agencies state they will require action over multiple years before they are fully implemented. For example, agencies officials told us the mid-term recommendation to expand sharing of information about network incidents and vulnerabilities with key allies is very broad, will require additional guidance in order to be fully implemented, and thus could take a number of years to complete. In addition, the mid-term recommendation to expand support for key education programs and research and development is an ongoing process that most likely will take several years to fully implement.

28

Results

While agencies have not yet been tasked with implementing specific recommendations, they have been working on other ongoing initiatives that address the 22 partially implemented recommendations. While these appear to be steps forward, the agencies were largely not able to provide milestones and plans that showed when and how implementation of the recommendations was to occur. Our analysis of the 22 partially implemented recommendations—described in attachment I—showed that 16 of the 22 did not have milestones and plans for implementation. More specifically, 4 of the 8 near-term recommendations and 12 of the 14 mid-term recommendations did not have such milestones and plans.

29

Results

Our extensive research and experience at federal agencies has shown that without clearly assigned roles and responsibilities and defined milestones and plans—including measures to assess progress and performance—agencies increase the risk that implementing such actions will not fully succeed.[10] Consequently, until roles and responsibilities are made clear and milestones and plans are defined, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.

[10]See, for example GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), GAO, *Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements,* GAO-04-842 (Washington, D.C.: Sept. 10, 2004), GAO, *Information Technology: Near-Term Effort to Automate Paper-Based Immigration Files Needs Planning Improvements*, GAO-06-375, (Washington, D.C.: Mar. 31, 2006), and GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338, (Washington, D.C: Mar. 5, 2010).

30

Conclusions

Although it has been over a year since the Executive Branch issued the results of its 2009 cyberspace policy review, agencies have yet to be assigned roles and responsibilities to implement a large majority of the near- and mid-term recommendations specified in the review. This notwithstanding, federal agencies appear to be making progress toward implementing the recommendations, but lack milestones, plans, and measures that are essential to ensuring successful recommendation implementation. The above shortcomings are attributable in part to the Cybersecurity Coordinator position being vacant for a critical period of time immediately following issuance of the recommendations. Consequently, going forward, it is essential that the Cybersecurity Coordinator address these shortfalls. Until then, there is increased risk the recommendations will not be successfully completed, which would unnecessarily place the country's cyber infrastructure at risk.

Recommendations for Executive Action

We recommend the Special Assistant to the President and Cybersecurity Coordinator, as part of implementing the 22 outstanding recommendations,

- designate roles and responsibilities for each recommendation, including which agencies are leading and supporting the effort; and
- develop milestones and plans, including measures to show agency implementation progress and performance, for the 16 recommendations identified in attachment I that lacked these key planning elements.

32

Agency Comments and Our Evaluation

In oral comments on a draft of this briefing, the Director for Cybersecurity within the office of the national Cybersecurity Coordinator generally concurred with our findings but took exception with our conclusions and recommendations. This official said he was in general agreement with the findings as they relate to the state of progress being made. However, with regard to our finding on the policy study recommendation to develop a national incident response plan, the Director said our statement in the briefing that the draft plan is not to be finalized until late summer 2010 and not to be tested until September 2010, while correct, created a negative and inaccurate picture that the effort is not on schedule. Our intent was not to imply that the effort was somehow lagging or behind schedule. Rather, it was to explain that the plan was under development and identify the work that remained to be performed.

Regarding our conclusions, the Director commented that he read the report to have a general implication and conclusion that progress is not being made. This official stated that contrary to this implication and conclusion, important progress is being made on all fronts. We agree that progress is being made and have stated this point throughout the briefing, including the conclusions section.

Agency Comments and Our Evaluation

With regard to our recommendations, the Director said he specifically disagreed with the recommendation on assigning roles and responsibilities. He noted that many of the policy review recommendations require contributions from multiple agency participants and those efforts are being coordinated through the ICI-IPC process. We acknowledge this comment but reiterate the evidence in our briefing that agencies participating in the ICI-IPC process said they had not been assigned roles and responsibilities with respect to recommendation implementation. Consequently, we stand by our recommendation.

The Director also provided technical comments—specifically with regard to recent progress on a national strategy for trusted identity in cyberspace that was issued since our draft briefing was transmitted for comment—which we incorporated where appropriate.

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Near-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.	The Administration is developing an updated national cyber strategy to replace the 2003 strategy. This effort is being lead by an ICI-IPC subcommittee called the Cyber-Operations sub-IPC. Although this effort is reportedly underway, Administration officials, including the Cybersecurity Coordinator, were unable to provide a draft strategy or milestones for when the updated strategy is to be finalized and issued.	No
Designate cybersecurity as one of the President's key management priorities and establish performance metrics.	The Administration has designated cybersecurity as one of the President's key management priorities. For example, in a May 2009 speech, President Obama declared the nation's cyber infrastructure as a national security priority. The Administration also proclaimed October 2009 as National Cybersecurity Awareness Month to promote the importance of cybersecurity and raise awareness. Additionally, in fiscal year 2011 budget, the Administration has proposed funding for cybersecurity initiatives. For example, for DHS, the Administration has requested $364 million in funding to support National Cyber Security Division[11] operations and CNCI efforts to secure and protect executive branch information systems. With regard to establishing performance metrics, the OMB is developing cybersecurity performance measures as part of its program assessment framework— a tool used by OMB in conjunction with agencies to improve programs by assessing factors (e.g., performance measures, strategic planning, evaluations) that affect performance to assist the federal government in achieving better results and informing funding decisions—but they are not scheduled to be completed until November 2010.	Yes

[11]The National Cyber Security Division, a component of DHS, serves as a national focal point for addressing cybersecurity and coordinating the implementation of cybersecurity efforts.

35

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Near-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Convene appropriate interagency mechanisms to conduct interagency-cleared legal analysis of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government.	The ICI-IPC is currently leading an interagency effort to provide legal analysis and clarify roles, responsibilities, and authorities to formulate policy guidance. Although these efforts are reported to be underway, Administration officials, including the Cybersecurity Coordinator, were unable to provide a target completion date for when the legal analysis would be completed and the guidance issued.	No
Initiate a national public awareness and education campaign to promote cybersecurity.	In mid-2009, the Administration formed an interagency education and training working group consisting of federal agencies, such as DHS, the Office of Personnel Management, and the Department of Education, to conduct a public awareness and education campaign. As part of this effort, NIST has taken on the overall coordination role for the education campaign—called the National Initiative for Cybersecurity Education—and is currently developing a strategic framework and plan of operation. The campaign consists of: (1) a national cybersecurity awareness campaign led by DHS; (2) cybersecurity education led by the Department of Education and the Office of Science and Technology Policy; (3) a federal workforce program led by the Office of Personnel Management; and (4) a national workforce training and professional development program lead by the DOD, DHS, and the Office of the Director of National Intelligence. Additionally, the President proclaimed October 2009 as National Cybersecurity Awareness Month to promote to the public that cybersecurity is a shared responsibility. While these activities are important efforts towards initiating a public awareness and education campaign, the Cybersecurity Coordinator stated that milestones and plans, among other things, have yet to be developed for completing initiation of this recommendation.	No

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Near-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Develop U.S. government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.	The Administration is developing an international cybersecurity policy framework to strengthen our international partnerships by addressing international threats, and establishing international norms of acceptable behavior in cyberspace. Nonetheless, the Administration was not able to provide a draft of the framework or a date for when the framework was to be completed. This finding is consistent with our recent report on this topic, which reported that coordination with international partners was a challenge to cybersecurity efforts and that the federal government did not have a formal strategy for coordinating outreach to international partners for the purposes of standards setting, law enforcement, and information sharing.[12] Consequently, we recommended that a coordinated approach be established for the federal government in conducting international outreach to address cyber security issues strategically.	No
Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.	In March 2010, DHS issued a draft cybersecurity incident response plan—called the National Cyber Incident Response Plan—that describes roles, responsibilities, and actions to prepare, respond, and recover from cyber incidents. This plan is part of the National Response Framework[13] issued by DHS in 2004 in response to the events in the aftermath of 9/11, which presents the guiding principles that enable first responders, decisionmakers, and support entities nationwide to provide a unified national response to disasters and emergences, including cybersecurity incidents. DHS reported that the plan included input from federal, state, and private sector partners. However, the draft plan is not to be finalized until late summer 2010. DHS does intend to test the plan (as part of a cyber incident exercise) in September 2010.	Yes

[12] GAO-10-338.
[13] The National Response Framework provides a structure for implementing a coordinated nationwide response to domestic incidents that range from accidents and natural disasters to actual or potential terrorist attacks.

37

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Near-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
In collaboration with other Executive Office of the President entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.	The Administration has efforts underway to develop a framework for research and development strategies. Specifically, according to officials within the Office of Science and Technology Policy, the office has recently begun developing such a framework. The framework is being developed as part of the office's Networking and Information Technology Research and Development program. As currently envisioned, the framework includes the following three key cybersecurity research and development themes: supporting security policies and security services for different types of cyber space interactions; deploying systems that are both diverse and changing; and developing cybersecurity incentives to create foundations for cybersecurity markets and establish meaningful metrics. The framework is expected to be finalized in 2011. Although the framework is under development, we recently reported[14] that the themes of the framework do not incorporate all priorities that should be included in a comprehensive national cybersecurity research and development agenda that is to serve as guidance for prioritizing federal cybersecurity research and development activities. Examples of priorities not incorporated in the framework include global-scale identity management, which was identified by DHS as a top problem that needs to be addressed, and computer forensics, which was identified by the private sector and several key government reports as a major area needing government focus. Consequently, we recommended that a comprehensive national research and development agenda be established by expanding the framework to, among other things, be consistent with the national cybersecurity strategy update that is currently under development.	Yes

[14] GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development,* GAO-10-466, (Washington, D.C: June 3, 2010).

38

Attachment I

Analysis of Partially Implemented Near-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties, leveraging privacy-enhancing technologies for the nation.	In July 2009, the Acting White House Cybersecurity Policy Advisor stated that work had begun on a framework to set priorities in the area of identity management. Specifically, NIST and other agencies are working with an ICI-IPC subcommittee (the Architecture, Research, and Development Sub-Committee of the Interagency Policy Committee) to develop an identity management strategy. In addition, NIST has other ongoing efforts in this area. For example, in November 2009, it held a workshop on identity management. More recently, in June 2010, the Administration released a draft of this strategy (entitled National Strategy for Trusted Identities in Cyberspace), that seeks to increase trust associated with the identities of individuals, organizations, services, and devices involved in financial and other types of online transactions. In addition, a stated aim of the draft strategy is to address privacy and civil liberty issues associated with identity management. However, the Administration does not plan to finalize the strategy until October 2010.	Yes

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.	As previously noted, the ICI-IPC is currently leading an interagency government legal analysis to clarify roles, responsibilities, and authorities to formulate policy guidance. Although these efforts are reported to be underway, Administration officials, including the Cybersecurity Coordinator, were unable to provide a target completion date for when the legal analysis would be completed and the guidance issued.	No
Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.	At the direction of the current Administration, the OMB is in the process of drafting an assessment framework for use with performance-based budgeting to aid agencies in pursuing their cybersecurity goals. According to OMB officials, they expect to have a finalized version of the assessment framework in November 2010.	Yes

40

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Expand support for key education programs and research and development to ensure the nation's continued ability to compete in the information age economy.	Several federal agencies have established efforts to expand support for education programs and research and development activities. For example, the National Science Foundation has annually funded a program (Scholarships For Service) which has the goal of increasing and strengthening the number of federal information assurance professionals protecting the government's critical information infrastructure. In addition, the National Science Foundation and DHS are part of the Science, Technology, Engineering, and Mathematics Education, also known as STEM, coalition which supports teachers and students in improving the way students learn science, mathematics, technology and engineering. Additionally, as stated above, the Administration established an interagency education and training working group that is currently supporting and promoting a public and education awareness campaign that includes developing formal cybersecurity education programs and national workforce training. Although these efforts appear to represent progress, the level of support envisioned by this recommendation has not been reached. Furthermore, agency officials stated that how and when the recommendation will be fully implemented has not been defined.	No

41

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the federal government.	Several federal agencies have efforts underway to expand and train the cybersecurity workforce. For example, as previously stated, in mid-2009, the Administration formed an interagency education and training working group consisting of federal agencies, such as NIST, DHS, the OMB, and the Department of Education, to conduct a public awareness and education campaign. The campaign consists of, among other things, a national workforce training and professional development program lead by the DOD, DHS, and the Office of the Director of National Intelligence. In addition, DHS is currently developing a Cyber Security Training Exercise Program across the federal government that is for officials working under Chief Information Officers. While these are steps towards implementing this recommendation, these officials were not able to provide us an overall strategy showing how the different federal agency efforts were integrated and coordinated to achieve the intended outcome of this recommendation nor could they provide a date for when such a strategy is to be developed and implemented.	No

42

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.	The DHS United States Computer Emergency Readiness Team (commonly referred to as US-CERT) coordinates the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communication networks. The US-CERT serves as a focal point for the government's interaction with federal and nonfederal entities on a 24-hour-a-day, 7-day-a-week basis regarding cyber-related analysis, warning, information sharing, major incident response, and national-level recovery efforts. It is also charged with aggregating and disseminating cybersecurity information to improve warning of and response to incidents, increasing coordination of response information, reducing vulnerabilities, and enhancing prevention and protection. Nonetheless, we reported[15] that the US-CERT faces a number of challenges that impede it from fully establishing cyber analysis and warning capabilities essential to coordinating the national effort to prepare for, prevent, and respond to cyber threats. In response to our recommendations to strengthen cyber analysis and warning capabilities, DHS has taken several steps. For example, the US-CERT has improved timeliness of strategic warnings by sharing information on a daily basis with personnel in key national coordination centers such as the White House Situation Room. However, DHS has yet to achieve situational awareness across the entire federal government and utilize predictive analysis across federal agencies and private networks and systems. The department has plans to address these items by 2012. In addition, no determination has been made with regard to the most efficient and effective mechanisms to obtain strategic warning, maintain situational awareness, and inform incident response capabilities, nor were agency officials able to provide us with a date for when such mechanisms would be determined.	No

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

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of research and development.	In August 2009, DHS, in collaboration with private and government coordinating councils established to protect information technology critical infrastructure (i.e., the Information Technology Sector Coordinating Council and the Information Technology Government Coordinating Council), issued the Information Technology Sector Baseline Risk Assessment.[16] The assessment identified risks to the information technology sector, provided risk management to enhance the security and resiliency of critical Information Technology Sector functions, including recovery planning and prioritization of research and development. While a positive step, this assessment falls short of meeting the recommendation because it is narrowly focused on the Information Technology Sector, and only addressed some but not all of the threat scenarios faced by the Information Technology Sector. In addition, DHS officials were not able to provide us milestones and plans for when and how this recommendation would be fully implemented.	No

[16] Department of Homeland Security, Information Technology Sector Coordinating Council, and Information Technology Government Coordinating Council, *Information Technology Sector Baseline Risk Assessment* (August 2009).

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents	We previously reported[17] that a process between the federal government and private sector exists for reporting cyber security incidents. Specifically, in 2009, we reported that this process, which is coordinated by US-CERT, included aspects of key success attributes relating to monitoring network activity, analyzing information, warning appropriate officials, and responding to threats. Although this process provided for aspects of each of the key attributes, we found that it does not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtains information from numerous external information sources, but has not established a baseline of our nation's critical network assets and operations. Furthermore, while US-CERT investigates whether identified anomalies constitute actual cyber threats or attacks as part of its analysis, it does not integrate its work into predictive analyses. Consequently, we recommended that DHS implement key success attributes and address challenges. Since then, DHS has addressed aspects of our recommendations. For example, it developed a plan for private sector partners to have increased access to secure communications at government facilities outside of the Washington, D.C. area. In addition, it has developed plans to address our remaining recommendations, including how to utilize predictive analysis across federal agencies and private networks and systems by the end of 2012. Further, as discussed above, DHS is currently working on the National Cyber Incident Response plan to establish a process for government and the private sector to respond to cyber and other types of incidents and expects to finalize the plan in late summer 2010.	Yes

[17]For example, see GAO-08-588.

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.	The federal government, through multiple agencies, has initiatives planned and underway that address this recommendation. For example, as previously mentioned, DHS has developed and established a process via US-CERT for reporting and sharing cybersecurity-related information. In addition, to foster and facilitate information sharing on cyber security issues among government agencies, DHS has established or funded several collaboration groups. Examples include DHS's Government Forum of Incident Response and Security Teams, and the Multi-State Information Sharing Analysis Center that coordinate cyber incident response for federal, state, and local governments. DHS has also established US-CERT programs that support collaboration throughout the federal government, such as the US-CERT Portal and Einstein programs that provide information sharing mechanisms for cyber-related information. With regard to the private sector, DHS has a program to coordinate information sharing among infrastructure sectors (e.g. energy, banking and finance, emergency services). As part of this program, DHS works to build trusted relationships; develop processes to facilitate information sharing; overcome barriers to information sharing; and clarify roles and responsibilities of the various government and private-sector entities involved in protecting critical infrastructures. Moreover, the National Science Foundation has supported research on information sharing under the Trustworthy Computing Program, a program aimed at facilitating information sharing while preserving privacy. While the above efforts are steps towards fostering information sharing, agency officials told us that they have not fully developed mechanisms for implementing this recommendation. In addition, they were not able to provide a milestones or plans for addressing these areas.	No

46

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality (a principle that advocates that Internet protocols be non-discriminatory and that content providers get equal treatment from Internet operators)	Federal agencies have multiple efforts planned and underway to develop emergency communications. Specifically, in 2009, we reported[18] that DHS and other federal agencies had issued a national emergency communications plan that aims to improve emergency communications nationwide by establishing operational targets to achieve a minimum level of interoperable communications, and dates by which federal, state, and tribal agencies are to achieve these goals. In our report, we recommended that DHS complete efforts to implement the plan, including establishing an emergency communications preparedness center to serve as a focal point and clearinghouse for intergovernmental emergency communications and information sharing during natural and man-made crises. Since then, DHS has been working with other agencies (e.g., the Federal Communications Commission) to implement the plan and establish the emergency center. More recently, we reported[19] that DHS was still working to establish the emergency communications preparedness center. For example, the department is currently in the process of defining the center's mission and addressing issues related to its legal authorities but department officials were not able to provide a date for when the center is to be made operational. (Continued on next page)	No

[18] For example, see GAO, *Emergency Communications: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts*, GAO-09-604 (Washington, D.C.: June 26, 2009).
[19] For example, see GAO, *Emergency Communications: Establishment of Emergency Communications Preparedness Center*, GAO-10-463R (Washington, D.C.: March 3, 2010).

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
(Continued)	In addition to these efforts, DHS has several ongoing programs that support emergency communications during crises. For example, the department has priority service programs including the Government Emergency Telecommunication Service, the Wireless Priority Service, and Telecommunications Service Priority, which provide capabilities to assure critical communications to support response, restoration, and assurance of critical services and functions. While these efforts represent progress toward implementing the recommendations, DHS officials told us the programs do not provide for network neutrality as called for in the recommendation. In addition, these officials were not able to provide milestones or plans for how the department was going to ensure network neutrality as part of these efforts or as a separate initiative.	

48

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.	Federal agencies have efforts planned and underway to (1) expand their sharing of information about network incidents and vulnerabilities with key allies and (2) seek arrangements to improve security while protecting civil liberties and privacy. For example, in June 2010, we reported[20] that the Federal Bureau of Investigation established bilateral and multilateral relationships with foreign countries to cooperate on cyber crime investigations, and is chair of a strategic alliance cyber crime working group—a multilateral effort with close United States allies to improve law enforcement cooperation. In addition, we reported[21] that DHS engaged in bilateral and multilateral relationships with foreign countries by (1) sharing information on issues of mutual concern and operations; (2) exchanging good practices; (3) collaborating on the development of mitigation measures; and (4) coordinating watch, warning and incident response efforts. Further, staff from the office of the Cybersecurity Coordinator has also stated that incident response sharing is occurring with key allies such as France and the United Kingdom. (Continued on next page)	No

[20] For example, see GAO, *Cyberspace: U.S. Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: June 28, 2010).
[21] GAO-10-606.

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
(Continued)	Although there are multiple efforts ongoing that address aspects of this recommendation, one key aspect—establishing a comprehensive national strategy that includes how to expand information sharing with allies and seek bilateral and multilateral arrangements to improve our economic and security interests—has not been completed. Specifically, in June 2010, we reported that federal agencies were challenged in this area because of this key missing guidance and, as such, we recommended that the Cybersecurity Coordinator, in collaboration with relevant federal agencies, develop a global national strategy. Federal agency officials were not able to tell us when such a strategy is to be developed.	

50

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.	Consistent with this recommendation, DOD has collaborated extensively with, and encouraged collaboration among universities and laboratories on research and technology initiatives. For example, under the Defense Multi-disciplinary University Research Initiative, the department has invested $118 million on research innovation (from fiscal year 2001 through fiscal year 2010) with 25 universities. The institutions taking part in these initiatives included the Universities of California, Maryland, and Carnegie Mellon, and the topics addressed include network surveillance, information assurance for wireless networks, and dynamic network management. In addition, DOD's Director for Defense Research and Engineering in conjunction with the Intelligence Advanced Research Projects conducted a study in 2009 on Cyber Security Technology Initiatives involving participants from 7 universities and 4 industrial entities. Further, DOD has held multiple national conferences and workshops, sponsored and hosted by the National Security Agency's National Information Assurance Research Laboratory that attract academic, industrial and government agencies. Although DOD has demonstrated collaboration with academia and industrial laboratories, these efforts do not fully meet the recommendation. Specifically, department officials told us their efforts did not include developing migration paths and incentives for rapid adoption of research and technology, as called for in the recommendation. The officials also were not able to provide a schedule or plan for addressing these areas.	No

51

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.	As co-chair of an ICI-IPC sub-committee[22] on international standards issues (i.e., the International sub-IPC's Standards Working Group), NIST has collaborated with other agencies, such as DOD, the Department of State, and the Federal Communications Commission, to define the federal government's goals and objectives for international cybersecurity technical standardization efforts. In particular, NIST is currently leading development of a working group white paper (entitled United States Government Strategic Objectives for International Cyber Security Standardization) that addresses, among other topics, cryptographic techniques, network security, privacy, and information security management systems. While these efforts will (1) propose long-term strategic goals and objectives for international cybersecurity standards, (2) document ongoing federal government international standards efforts, and (3) identify gaps in participation, NIST officials told us that no final date has been set for completion of this document.	No

[22] Co-chaired with the National Security Agency.

52

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Implement for high-value activities (e.g., The Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.	As noted previously, NIST is helping to develop a federal identity management strategy that is to serve as a guide for federal agencies to develop and implement interoperable identity management systems. Specifically, NIST and other agencies are working with an ICI-IPC subcommittee (i.e., the Architecture, Research, and Development Sub-Committee of the Interagency Policy Committee) to develop an identity management strategy as part of a national strategy document being developed on securing online transactions. In addition, NIST is participating in committees of the American National Standards Institute, the International Organization for Standardization, and the International Electrotechnical Commission to develop standards to support identity management systems that address topics including smart cards, cyber security, and biometrics. Moreover, in June 2010, the Administration released a draft of this strategy (entitled National Strategy for Trusted Identities in Cyberspace), that seeks to increase trust associated with the identities of individuals, organizations, services, and devices involved in financial and other types of online transactions. However the Administration does not plan to finalize the strategy until October 2010. According to NIST officials, they do not know precisely when all these activities are to be completed and were not able to provide milestones and plans for when and how the recommendation is to be fully implemented.	No

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.	Federal agencies have efforts—commonly referred to as supply chain programs—planned and underway with the stated goals of refining their procurement strategies and improving market incentives for secure products, security innovation, and secure services. For example, as part of the CNCI initiative on developing an approach for global supply chain risk management, DHS has developed a (1) policy outline identifying short-term solutions that federal agencies can take to establish a supply chain program, and (2) training plan to implement the policy. The department is also developing another policy document that is to identify longer-term solutions and is to include recommendations to the OMB for establishing a governmentwide supply chain program that incorporates security benchmarks to evaluate suppliers, their products, and services. This policy is scheduled to be completed by the end of September 2010. In addition, NIST stated that as part of the CNCI initiative on supply chain management, it has assisted DHS and DOD in developing lifecycle process and standard documents that incorporate supply chain risk management controls, the departments plan to complete the documents by September 2010. NIST also said that it provided technical assistance to an ICI-IPC subgroup in developing an interagency report and methodology on how supply change risk management is to be implemented in acquiring federal civilian information systems software and hardware. The draft report is to be issued the end of June 2010. (Continued on next page)	No

GAO
Accountability * Integrity * Reliability

Attachment I

Analysis of Partially Implemented Mid-term Recommendations, Including Whether Milestones and Plans Were Developed

Recommendation	Description of Why Status is Partially Implemented	Milestones/Plans
(Continued)	Although agency officials have taken steps to develop and implement a supply chain strategy consistent with this recommendation, the process is not yet implemented. In addition, agency officials were not able to describe how their efforts were going to improve market incentives for secure products, security innovation, and secure managed services. Further, they were not able to provide milestones or plans for when the missing elements were to be addressed and when the recommendation was to be fully implemented.	

55

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 contact name above, individuals making contributions to this report included: Gary Mountjoy, Assistant Director; Gerard Aflague; 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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu