United States Government Accountability Office

GAO

Report to Congressional Addressees

February 2013

CYBERSECURITY

National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented

February 2013

CYBERSECURITY

National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented

Highlights of GAO-13-187, a report to congressional addressees

Why GAO Did This Study

Cyber attacks could have a potentially devastating impact on the nation's computer systems and networks, disrupting the operations of government and businesses and the lives of private individuals. Increasingly sophisticated cyber threats have underscored the need to manage and bolster the cybersecurity of key government systems as well as the nation's critical infrastructure. GAO has designated federal information security as a government-wide high-risk area since 1997, and in 2003 expanded it to

milestones and performance measures at the strategic level is mirrored in similar shortcomings within key government programs that are part of the government-wide strategy. The DHS inspector general, for example, recommended in 2011 that DHS develop and implement performance measures to be used to track and evaluate the effectiveness of actions defined in its strategic implementation plan. As of January 2012, DHS had not yet developed the performance measures but planned to do so.

- Cost and resources. While past strategy documents linked certain activities to budget submissions, none have fully addressed cost and resources, including justifying the required investment, which is critical to gaining support for implementation. In addition, none provided full assessments of anticipated costs and how resources might be allocated to address them.
- Roles and responsibilities . Cybersecurity strategy documents have assigned high-level roles and responsibilities but have left important details unclear. Several GAO reports have likewise demonstrated that the roles and responsibilities of key agencies charged with protecting the nation's cyber assets are inadequately defined. For example, the chartering directives for several offices within the Department of Defense assign overlapping roles and responsibilities for preparing for and responding to domestic cyber incidents. In an October 2012 report, GAO recommended that the department update its guidance on preparing for and responding to domestic cyber incidents to include a description of its roles and responsibilities. In addition, it is unclear how OMB and DHS are to share oversight of individual departments and agencies. While the law gives OMB responsibility for oversight of federal government information security, OMB transferred several of its oversight responsibilities to DHS. Both DHS and OMB have issued annual FISMA reporting instructions to agencies, which could create confusion among agency officials because the instructions vary in content. Clarifying oversight responsibilities is a topic that could be effectively addressed through legislation.
- Linkage with other key strategy documents . Existing cybersecurity strategy documents vary in terms of priorities and structure, and do not specify how they link to or supersede other documents, nor do they describe how they fit into an overarching national cybersecurity strategy. For example, in 2012, the administration determined that trusted Internet connections, continuous monitoring, and strong authentication should be cross-agency priorities, but no explanation was given as to how these three relate to priorities previously established in other strategy documents.

The many continuing cybersecurity challenges faced by the government highlight the need for a clearly defined oversight process to ensure agencies are held accountable for implementing effective information security programs. Further, until an overarching national cybersecurity strategy is developed that addresses all key elements of desirable characteristics, overall progress in achieving the government's objectives is likely to remain limited.

What GAO Recommends

To address missing elements in the national cybersecurity strategy, such as milestones and performance measures, cost and resources, roles and responsibilities, and linkage with other key strategy documents, GAO recommends that the White House Cybersecurity Coordinator develop an overarching federal cybersecurity strategy that includes all key elements of the desirable characteristics of a national strategy. Such a strategy would provide a more effective framework for implementing cybersecurity activities and better ensure that such activities will lead to progress in cybersecurity.

This strategy should also better ensure that federal departments and agencies are held accountable for making significant improvements in cybersecurity challenge areas, including designing and implementing risk-based programs; detecting, responding to, and mitigating cyber incidents; promoting education, awareness, and workforce planning; promoting R&D; and addressing international cybersecurity challenges. To address these issues, the strategy should (1) clarify how OMB will oversee agency implementation of requirements for effective risk management processes and (2) establish a roadmap for making significant improvements in cybersecurity challenge areas where previous recommendations have not been fully addressed.

Further, to address ambiguities in roles and responsibilities that have resulted from recent executive branch actions, GAO believes Congress should consider legislation to better define roles and responsibilities for implementing and overseeing federal information security programs and for protecting the nation's critical cyber assets.

In its comments, the Executive Office of the President agreed that more needs to be done to develop a coherent and comprehensive strategy on cybersecurity but did not believe producing another strategy document would be beneficial. However, GAO believes an overarching strategy document that includes milestones and performance measures, cost and resources, roles and responsibilities, and linkage with other key strategy documents would provide a more effective framework for implementing cybersecurity activities. The Executive Office of the President also agreed that Congress should consider enhanced cybersecurity legislation.

Contents

Letter		1
	Background	3
	Federal Strategy Has Evolved Over Time but Is Not Fully Defined	19
	The Federal Government Continues to Face Challenges in Implementing Cybersecurity that Could Be Addressed by an Effective Strategy	36
	Conclusions	81
	Recommendations for Executive Action	82
	Matter for Congressional Consideration	83
	Agency Comments and Our Evaluation	83
Appendix I	Objectives, Scope, and Methodology	88
Appendix II	List of Panel and Survey Participants	91
Appendix III	Comments from the Department of Homeland Security	95
Appendix IV	GAO Contacts and Staff Acknowledgments	98
Related GAO Products		99

Tables

Table 1: Sources of Adversarial Threats to Cybersecurity	5
Table 2: Types of Cyber Attacks	6
Table 3: Summary of Desirable Characteristics for a National Strategy	29

Figures

Figure 1: Incidents Reported to US-CERT: Fiscal Years 2006-2012	8
Figure 2: Incidents Reported to US-CERT by Federal Agencies in Fiscal Year 2012 by Category	9

e r r rPgi t Gt 7ee yeAy-8Qy ui 1ng

Figure 3: Evolution of National Strategies Related to Cybersecurity 20
Figure 4: NIST Risk Management Process Applied Across the Tiers 38
Figure 5: Percentage of Continuous Monitoring Capabilities Reported by Agencies in Fiscal Year 2011 44

e r r rPgi t Gt 7ee yeAy-8Qy ui 1tg

Appendix V

CIO	chief information officer
CNCI	Comprehensive National Cybersecurity Initiative
CS&C	Office of Cybersecurity and Communication
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
E^3A	EINSTEIN 3 Accelerated
FISMA	Federal Information Security Management Act
GPRA	Government Performance and Results Act
HHS	Department of Health and Human Services
HSPD-7	Homeland Security Presidential Directive 7
ISAC	Information Sharing and Analysis Center
JACKE	Joint Agency Cyber Knowledge Exchange
NASA	National Aeronautics and Space Administration
NCCIC	National Cybersecurity and Communications Integration Center
NICE	National Initiative for Cybersecurity Education
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NITRD	Subcommittee on Networking and Information Technology Research and Development
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
R&D	research and development
TSP	Thrift Savings Plan
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VA	Department of Veterans Affairs

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

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

February 14, 2013

Congressional Addressees

The pervasive use of the Internet has revolutionized the way that our government, our nation, and the rest of the world communicates and conducts business. While the benefits have been enormous, this widespread connectivity also poses significant risks to the government's and our nation's computer systems and networks as well as the critical operations and key infrastructures they support. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, can allow unauthorized individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for potentially malicious purposes, including fraud or sabotage. Increasingly sophisticated cyber threats have underscored the need to manage and bolster the cybersecurity of key government systems as well as the nation's critical infrastructure.[1]

Federal law and policy call for a risk-based approach to managing cybersecurity within the government and also specify activities to enhance the cybersecurity of public and private infrastructures that are essential to national security, national economic security, and public health and safety.[2] Over the last 12 years, the federal government has developed a number of strategies and plans for addressing cybersecurity based on this legal framework, including the National Strategy to Secure Cyberspace, issued in February 2003, and subsequent plans and strategies that address specific sectors, issues, and revised priorities.

We performed our work on the initiative of the U.S. Comptroller General to evaluate the federal government's cybersecurity strategies and understand the status of federal cybersecurity efforts to address challenges in establishing a strategic cybersecurity approach. Our objectives were to (1) determine the extent to which the national

[1]Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security.

[2]This includes the Federal Information Security Management Act of 2002 (FISMA), the Homeland Security Act of 2002, and the Homeland Security Presidential Directive 7, among other laws and directives.

e r r rPg a t Gt 1 7ee yeAy-8Qy ui 1g

cybersecurity strategy includes key desirable characteristics of effective strategies, and (2) identify challenges faced by the federal government in addressing a strategic approach to cybersecurity.

To address our objectives, we analyzed key documents that reflect the federal government's evolving cybersecurity strategy, as well as other pertinent national strategies to determine the extent to which they included GAO's key desirable characteristics of a national strategy. In addition, we reviewed our previous reports and reports by agency inspectors general to identify key challenge areas. We also interviewed representatives from federal agencies with government-wide responsibilities for cybersecurity, including the Executive Office of the President, Office of Management and Budget (OMB), the Departments of Homeland Security (DHS) and Defense (DOD), and the National Institute of Standards and Technology (NIST), to obtain their views on cybersecurity issues as well as updated information about strategic initiatives. We also obtained expert perspective on key issues through use of two expert panels as well as surveys of cybersecurity experts and the chief information officers (CIO) of the 24 major federal agencies covered by the Chief Financial Officers Act.[3]

We conducted this performance audit from April 2012 to February 2013 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. A full description of our objectives, scope, and methodology can be found in appendix I. In addition, the names of cybersecurity and information management experts participating in our two expert panels, as well as participants in our expert survey and CIO survey, can be found in appendix II.

[3]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

Background

Threats to systems supporting critical infrastructure and federal information systems are evolving and growing. Advanced persistent threats—where adversaries that possess sophisticated levels of expertise and significant resources to pursue its objectives repeatedly over an extended period of time—pose increasing risks. In 2009, the President declared the cyber threat to be "[o]ne of the most serious economic and national security challenges we face as a nation" and stated that "America's economic prosperity in the 21st century will depend on cybersecurity."[4] The Director of National Intelligence has also warned of the increasing globalization of cyber attacks, including those carried out by foreign militaries or organized international crime. In January 2012, he testified that such threats pose a critical national and economic security concern.[5] To further highlight the importance of the threat, on October 11, 2012, the Secretary of Defense stated that the collective result of attacks on our nation's critical infrastructure could be "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."[6] These growing and evolving threats can potentially affect all segments of our society, including individuals, private businesses, government agencies, and other entities. We have identified the protection of federal information systems as a high-risk area for the government since 1997.[7] In 2003, this high-risk area was expanded to include protecting systems supporting our nation's critical infrastructure. Each year since that time, GAO has issued multiple reports detailing weaknesses in federal information security programs and making recommendations to address them. A list of key GAO products can be found at the end of this report.

Sources of Threats and Attack Methods Vary

The evolving array of cyber-based threats facing the nation pose threats to national security, commerce and intellectual property, and individuals.

[4]President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure" (Washington, D.C.: May 29, 2009).

[5]James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence" (January 31, 2012).

[6]Secretary of Defense Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (New York, NY: Oct. 11, 2012).

[7]See GAO, High Risk Series: An Update, GAO-11-278 (Washington, D.C.: February 2011).

- Threats to national security include those aimed against the systems and networks of the U.S. government, including the U.S. military, as well as private companies that support government activities or control critical infrastructure. These threats may be intended to cause harm for monetary gain or political or military advantage and can result, among other things, in the disclosure of classified information or the disruption of operations supporting critical infrastructure, national defense, or emergency services.

- Threats to commerce and intellectual property include those aimed at obtaining the confidential intellectual property of private companies, the U.S. government, or individuals with the aim of using that intellectual property for economic gain. For example, product specifications may be stolen to facilitate counterfeiting and piracy or to gain a competitive edge over a commercial rival. In some cases, theft of intellectual property may also have national security repercussions, as when designs for weapon systems are compromised.

- Threats to individuals include those that lead to the unauthorized disclosure of personally identifiable information, such as taxpayer data, Social Security numbers, credit and debit card information, or medical records. The disclosure of such information could cause harm to individuals, such as identity theft, financial loss, and embarrassment.

The sources of these threats vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. Table 1 shows common sources of adversarial cybersecurity threats.

e r r rPg a t t 7ee yeAy-8 ui 1

Bot-network operators	Bot-network operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive viruses and worms have harmed files and hard drives, and reportedly have even caused physical damage to critical infrastructure, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

These sources of cybersecurity threats make use of various techniques, or attacks that may compromise information or adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Table 2 provides descriptions of common types of cyber attacks.

Table 2: Key Types of Cyber Attacks and Descriptions of Each

Type of attack	Description
Cross-site scripting	An attack that uses third-party web resources to run a script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike viruses, worms do not require human involvement to propagate.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

The unique nature of cyber-based attacks can vastly enhance their reach and impact, resulting in the loss of sensitive information and damage to economic and national security, the loss of privacy, identity theft, or the compromise of proprietary information or intellectual property. The increasing number of incidents reported by federal agencies, and the

recently reported cyber-based attacks against individuals, businesses, critical infrastructures, and government organizations have further underscored the need to manage and bolster the cybersecurity of our government's information systems and our nation's critical infrastructures.

Number of Incidents Reported by Federal Agencies Continues to Rise, and Recently Reported Incidents Illustrate Potential Impact

Federal agencies have reported increasing numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. The increasing risks to federal systems are demonstrated by the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. As shown in figure 1, over the past 6 years, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) has increased from 5,503 in fiscal year 2006 to 48,562 incidents in fiscal year 2012, an increase of 782 percent. These incidents include, among others, the installation of malware,[8] improper use of computing resources, and unauthorized access to systems.

[8]Malware is malicious software and is defined as programs that are designed to carry out annoying or harmful actions. Once installed, malware can often masquerade as useful programs or be embedded into useful programs so that users are induced into activating the program, spreading itself onto other devices.

Of the incidents occurring in 2012 (not including those that were reported as under investigation), improper usage,[9] malicious code, and unauthorized access were the most widely reported types across the federal government. As indicated in figure 2, which includes a breakout of incidents reported to US-CERT by agencies in fiscal year 2012, improper usage accounted for 20 percent of total incidents reported by agencies.

[9]An incident is categorized as “improper usage” if a person violates acceptable computing use policies.

The major cybersecurity initiatives and strategy documents that have been developed over the last 12 years are discussed below.

The National Plan for Information Systems Protection

In 2000, President Clinton issued the National Plan for Information Systems Protection. The plan was intended as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. It focused on federal efforts to protect the nation's critical cyber-based infrastructures. It identified risks associated with our nation's dependence on computers and networks for critical services; recognized the need for the federal government to take a lead role in addressing critical infrastructure risks; and outlined key concepts and general initiatives to assist in achieving its goals. The plan identified specific action items and milestones for 10 component programs that were aimed at addressing the need to prepare for and prevent cyber attacks, detect and respond to attacks when they occur, and build strong foundations to support these efforts.

The National Strategy to Secure Cyberspace

In 2003, the National Strategy to Secure Cyberspace was released. It was also intended to provide a framework for organizing and prioritizing efforts to protect cyberspace and was organized according to five national priorities, with major actions and initiatives identified for each. These priorities were

- a National Cyberspace Security Response System,
- a National Cyberspace Security Threat and Vulnerability Reduction Program,
- a National Cyberspace Security Awareness and Training Program,
- Securing Governments' Cyberspace, and
- National Security and International Cyberspace Security Cooperation.

In describing the threats to and vulnerabilities of cyberspace, the strategy highlighted the potential for damage to U.S. information systems from attacks by terrorist organizations.

Although it is unclear whether the 2003 strategy replaced the 2000 plan or was meant to be a supplemental document, the priorities of the 2003 strategy are similar to those of the 2000 document. For example, the 2003 strategy's priority of establishing a national cyberspace security threat and vulnerability reduction program aligns with the 2000 plan's

programs related to identifying critical infrastructure assets and shared interdependencies, addressing vulnerabilities, and detecting attacks and unauthorized intrusions. In addition, the 2003 strategy's priority of minimizing damage and recovery time from cyber attacks aligns with the 2000 plan's program related to creating capabilities for response, reconstitution, and recovery. The 2000 plan also included programs addressing awareness and training, cyber-related counterintelligence and law enforcement, international cooperation, and research and development, similar to the 2003 strategy.

The Comprehensive National Cybersecurity Initiative

In 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23, establishing the Comprehensive National Cybersecurity Initiative (CNCI), a set of 12 projects aimed at safeguarding executive branch information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. The 12 projects were the following:

1. Reduce and consolidate external access points with the goal of limiting points of access to the Internet for executive branch civilian agencies.
2. Deploy passive sensors across executive branch civilian systems that have the ability to scan the content of Internet packets to determine whether they contain malicious code.
3. Pursue deployment of an intrusion prevention system that will allow for real-time prevention capabilities that will assess and block harmful code.
4. Coordinate and redirect research and development (R&D) efforts with a focus on coordinating both classified and unclassified R&D for cybersecurity.
5. Connect current cyber centers to enhance cyber situational awareness and lead to greater integration and understanding of the cyber threat.
6. Develop a government-wide cyber counterintelligence plan by improving the security of the physical and electromagnetic integrity of U.S. networks.

8. Increase the security of classified networks to reduce the risk of information they contain being disclosed.
9. Expand education efforts by constructing a comprehensive federal cyber education and training program, with attention to offensive and defensive skills and capabilities.
10. Define and develop enduring leap-ahead technology, strategies, and programs by investing in high-risk, high-reward research and development and by working with both private sector and international partners.
11. Define and develop enduring deterrence strategies and programs that focus on reducing vulnerabilities and deter interference and attacks in cyberspace.
12. Develop a multipronged approach for global supply chain risk management while seeking to better manage the federal government's global supply chain.
13. Define the federal role for extending cyber security into critical infrastructure domains and seek to define new mechanisms for the federal government and industry to work together to protect the nation's critical infrastructure.

The CNCI's projects are generally consistent with both the 2000 strategy and the 2003 strategy, while also introducing new priorities. For example, all three strategy documents address counterintelligence, education and awareness, research and development, reducing vulnerabilities, and public-private partnerships. However, the CNCI introduces additional priorities for the security of classified networks and global supply chain risk management, and it does not include programs to address response, reconstitution, and recovery or international cooperation, as in the previous strategies.

White House Cyberspace Policy Review

Shortly after taking office in 2009, President Obama ordered a thorough review of the federal government's efforts to defend the nation's information and communications infrastructure as well as the development of a comprehensive approach to cybersecurity. The White House Cyberspace Policy Review, released in May 2009, was the result. It recommended that the President appoint a national cybersecurity coordinator, which was completed in December 2009. It also

recommended, among many other things, that a coherent unified policy guidance be developed that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government; a cybersecurity incident response plan be prepared; a national public awareness and education campaign be initiated that promotes cybersecurity; and a framework for research and development strategies be created. According to the policy review, President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national strategy. In addition, the CNCI initiatives were to play a key role in supporting the achievement of many of the policy review's recommendations.

National Strategy for Trusted Identities in Cyberspace

The National Strategy for Trusted Identities in Cyberspace[31] is one of several strategy documents that are subordinate to the government's overall cybersecurity strategy and focuses on specific areas of concern. Specifically, this strategy aims at improving the security of online transactions by strengthening the way identities are established and confirmed. The strategy envisions secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. In order to fulfill its vision, the strategy calls for

- developing a comprehensive Identity Ecosystem[32] Framework,
- building and implementing interoperable identity solutions,
- enhancing confidence and willingness to participate in the Identity Ecosystem, and
- ensuring the long-term success and viability of the Identity Ecosystem.

[31]The White House, National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy (Washington, D.C.: April 2011).

[32]The strategy defines an "Identity Ecosystem" as an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices.

The first two goals focus on designing and building the necessary policy and technology to deliver trusted online services. The third goal encourages adoption, including the use of education and awareness efforts. The fourth goal promotes the continued development and enhancement of the Identity Ecosystem. For each goal, there are objectives that enable the achievement of the goal by addressing barriers in the current environment. The strategy states that these goals will require the active collaboration of all levels of government and the private sector. The private sector is seen as the primary developer, implementer, owner, and operator of the Identity Ecosystem, and the federal government's role is to "enable" the private sector and lead by example through the early adoption and provision of Identity Ecosystem services.

Strategic Plan for Cybersecurity Research and Development

In response to the R&D-related recommendations in the White House Cyberspace Policy Review, the Office of Science and Technology Policy (OSTP)[33] issued the first cybersecurity R&D strategic plan[34] in December 2011, which defines a set of interrelated priorities for government agencies conducting or sponsoring cybersecurity R&D. This document is another of the subordinate strategy documents that address specific areas of concern. The priorities defined in the plan are organized into four goals—inducing change, developing scientific foundations, maximizing research impact, and accelerating transition to practice—that are aimed at limiting current cyberspace deficiencies, precluding future problems, and expediting the infusion of research accomplishments in the marketplace. Specifically, the plan identifies what research is needed to reduce cyber attacks. It includes the following themes:

- building a secure software system that is resilient to attacks;
- supporting security policies and security services for different types of cyberspace interactions;
- deploying systems that are both diverse and changing, to increase complexity and costs for attackers and system resiliency; and

[33]OSTP, an office within the Executive Office of the President, advises the President on science and technology issues. It also coordinates related polices and R&D strategies across federal agencies, including through the National Science and Technology Council.

[34]National Science and Technology Council, Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (Washington, D.C.: Dec. 6, 2011).

- developing cybersecurity incentives to create foundations for cybersecurity markets, establish meaningful metrics, and promote economically sound and secure practices.

International Strategy for Cyberspace

Like the strategies for trusted cyberspace identities and cyberspace R&D, the International Strategy for Cyberspace,[35] released by the White House in May 2011, is a subordinate strategy document that addresses a specific area of concern. The International Strategy for Cyberspace is intended to be a roadmap for better definition and coordination of U.S. international cyberspace policy. According to the strategy, in order to reach the goal of working internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure, the government is to build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace. The strategy stated that these cyberspace norms should be supported by principles such as upholding fundamental freedoms, respect for property, valuing privacy, protection from crime, and the right of self-defense. The strategy also included seven interdependent focus areas:

1. Economy: Promoting International Standards and Innovative, Open Markets.
2. Protecting our Networks: Enhancing Security Reliability and Resiliency.
3. Law Enforcement: Extending Collaboration and the Rule of Law.
4. Military: Preparing for 21st Century Security Challenges.
5. Internet Governance: Promoting Effective and Inclusive Structures.
6. International Development: Building Capacity, Security, and Prosperity.
7. Internet Freedom: Supporting Fundamental Freedoms and Privacy.

[35]The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, D.C.: May 2011).

2012 Cross-Agency Priority Goals

In a March 2012 blog post, the White House Cybersecurity Coordinator announced that his office, in coordination with experts from DHS, DOD, NIST, and OMB, had identified three priority areas for improvement within federal cybersecurity:

- Consolidate external telecommunication connections and ensure a set of baseline security capabilities for situational awareness and enhanced monitoring.
- Continuously monitor transition the otherwise static security control assessment and authorization process into a dynamic risk mitigation program that provides essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk management decisions based on increased situational awareness.
- Increase the use of federal smartcard credentials such as Personal Identity Verification and Common Access Cards that provide multifactor authentication and digital signature and encryption capabilities, authorizing users to access federal information systems with a higher level of assurance.

According to the post, these priorities were selected to focus federal department and agency cybersecurity efforts on implementing the most cost-effective and efficient cybersecurity controls for federal information system security. To support the implementation of these priorities, cybersecurity was included among a limited number of cross-agency priority goals, as required to be established under the GPRA Modernization Act of 2010.[36] The cybersecurity goal was to achieve 95 percent use of critical cybersecurity capabilities on federal executive branch information systems by the end of 2014, including the three priorities mentioned above. The White House Cybersecurity Coordinator was designated as the goal leader, but according to one White House website, http://www.performance.gov, DHS was tasked with leading the government-wide coordination efforts to implement the goal. The administration's priorities were included in its fiscal year 2011 FISMA report to Congress. In addition, both OMB and DHS FISMA reporting

[36]Pub. L. No. 111-352, 124 Stat. 3866, 3873 (2011).

instructions require federal agencies to report on progress in meeting those priorities in their 2012 FISMA reports.

There are a number of implementation plans aimed at executing various aspects of the national strategy. For example, the National Infrastructure Protection Plan (NIPP)[37] describes DHS's overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. The goal of the NIPP is to prevent, deter, neutralize, or mitigate the effects of terrorist attacks on our nation's critical infrastructure and to strengthen national preparedness, timely response, and rapid recovery of critical infrastructure in the event of an attack, natural disaster, or other emergency. The NIPP's objectives include understanding and sharing information about terrorist threats and other hazards with critical infrastructure partners; building partnerships to share information and implement critical infrastructure protection programs; implementing a long-term risk management program; and maximizing the efficient use of resources for critical infrastructure protection, restoration, and recovery.

No Overarching Cybersecurity Strategy Has Been Developed

While various subordinate strategies and implementation plans focusing on specific cybersecurity issues have been released in the past few years, no overarching national cybersecurity strategy document has been prepared that synthesizes the relevant portions of these documents or provides a comprehensive description of the current strategy. According to officials at the Executive Office of the President, the current national cybersecurity strategy consists of several documents and statements issued at different times, including the 2003 strategy, which is now almost a decade old, the 2009 White House policy review, and subordinate strategies such as the R&D strategy and the international strategy. Also implicitly included in the national strategy are the modifications made when the CNCI was introduced in 2008 and the 2012 statement regarding cross-agency priority goals.

Despite the fact that no overarching document has been created, the White House has asserted that the national strategy has in fact been updated. We reported in October 2010 that a committee had been formed

[37]DHS, National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency (Washington, D.C.: January 2009).

to prepare an update to the 2003 strategy in response to the recommendation of the 2009 policy review.[38] However, no updated strategy document has been issued. In May 2011, the White House announced that it had completed all the near-term actions outlined in the 2009 policy review, including the update to the 2003 national strategy. According to the administration's fact sheet on cybersecurity accomplishments,[39] the 2009 policy review itself serves as the updated strategy. The fact sheet stated that the direction and needs highlighted in the Cyberspace Policy Review and the previous national cybersecurity strategy were still relevant, and it noted that the administration had updated its strategy on two subordinate cyber issues, identity management and international engagement. However, these actions do not fulfill the recommendation that an updated strategy be prepared for the President's approval. As a result, no overarching strategy exists to show how the various goals and activities articulated in current documents form an integrated strategic approach.

Useful Strategies Should Include Desirable Characteristics

In 2004 we identified a set of desirable characteristics that can enhance the usefulness of national strategies as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability.[40] Table 3 provides a summary of the six characteristics.

Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.
Problem definition and risk assessment	Addresses the particular national problems and threats the strategy is directed toward.
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve and steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.

[38]GAO, Cyberspace Policy: Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed, GAO-11-24 (Washington, D.C.: Oct. 6, 2010).

[39]The White House, "Fact Sheet: The Administration's Cybersecurity Accomplishments" (May 12, 2011), accessed on July 26, 2012, http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments.

[40]GAO, Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

Desirable characteristic	Description
Resources, investments, and risk management	Addresses what implementation of the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.
Linkage to other strategies and implementation	Addresses how a national strategy relates to other strategies' goals, objectives, and activities, and to subordinate levels of government and their plans to implement the strategy.

Source: GAO.

We believe that including all the key elements of these characteristics in a national strategy would provide valuable direction to responsible parties for developing and implementing the strategy, enhance its usefulness as guidance for resource and policy decision makers, and better ensure accountability.

Federal Cybersecurity Strategy Documents Have Not Always Included Key Elements of Desirable Characteristics

The government's cybersecurity strategy documents have generally addressed several of the desirable characteristics of national strategies, but lacked certain key elements. For example, the 2009 White House Cyberspace Policy Review, the Strategy for Trusted Identities in Cyberspace, and the Strategic Plan for the Federal Cybersecurity Research and Development Program addressed purpose, scope, and methodology. In addition, all the documents included the problem definition aspect of "problem definition and risk assessment." Likewise, the documents all generally included goals, subordinate objectives, and activities, which are key elements of the "goals, subordinate objectives, activities, and performance measures" characteristic. However, certain elements of the characteristics were missing from most, if not all, of the documents we reviewed. The key elements that were generally missing from these documents include (1) milestones and performance measures, (2) cost and resources, (3) roles and responsibilities, and (4) linkage with other strategy documents.

Milestones and Performance Measures

Milestones and performance measures were generally not included in strategy documents, appearing only in limited circumstances within subordinate strategies and initiatives. For example, the Cross-Agency Priority Goals for Cybersecurity and the National Strategy for Trusted

Identities in Cyberspace,[41] which represent only a portion of the national strategy, included milestones for achieving their goals. In addition, the progress in implementing the Cross-Agency Priority Goals for Cybersecurity is tracked through FISMA reports submitted by agencies and their inspectors general. However, in general, the documents and initiatives that currently contribute to the government's overall cybersecurity strategy do not include milestones or performance measures for tracking progress in accomplishing stated goals and objectives. For example, the 2003 National Strategy to Secure Cyberspace included no milestones or performance measures for addressing the five priority areas it defined. Likewise, other documents generally did not include either milestones for implementation of the strategy or outcome-related performance measures to gauge success.

The lack of milestones and performance measures at the strategic level is mirrored in similar shortcomings within key government programs that are part of the government-wide strategy. For example, the DHS inspector general reported in 2011 that the DHS Cybersecurity and Communications (CS&C) office had not yet developed objective, quantifiable performance measures to determine whether it was meeting its mission to secure cyberspace and protect critical infrastructures.[42] Additionally, the inspector general reported that CS&C was not able to track its progress efficiently and effectively in addressing the actions outlined in the 2003 National Cybersecurity Strategy or achieving the goals outlined in the NIPP. Accordingly, the inspector general recommended that CS&C develop and implement performance measures to be used to track and evaluate the effectiveness of actions defined in its strategic implementation plan. The inspector general also recommended that management use these measures to assess CS&C's overall progress in attaining its strategic goals and milestones. DHS officials stated that, as of January 2012, CS&C had not yet developed objective performance criteria and measures, and that development of these will begin once the CS&C strategic implementation plan is completed.

[41]The National Strategy for Trusted Identities in Cyberspace includes interim benchmarks (3-5 years) and longer-term benchmarks (10 years) for determining whether the strategy was successful.

[42]DHS Office of Inspector General, Planning, Management, and Systems Issues Hinder DHS' Efforts to Protect Cyberspace and the Nation's Cyber Infrastructure, OIG-11-89 (Washington, D.C.: June 2011).

Many of the experts we consulted cited a lack of accountability as one of the root causes for the slow progress in implementing the nation's cybersecurity goals and objectives. Specifically, cybersecurity and information management experts stated that the inability of the federal government to make progress in addressing persistent weaknesses within its risk-based security framework can be associated with the lack of performance measures and monitoring to assess whether security objectives are being achieved. Without establishing milestones or performance measures in its national strategy, the government lacks a means to ensure priority goals and objectives are accomplished and responsible parties are held accountable.

Cost and Resources

Though the 2000 plan and the 2003 strategy linked some investments to the annual budget, the strategy documents generally did not include an analysis of the cost of planned activities or the source and type of resources needed to carry out the strategy's goals and objectives. The 2000 National Plan for Information Systems Protection identified resources for certain cybersecurity activities, and the 2003 National Strategy to Secure Cyberspace linked some of its investment requests—such as completing a cyber incident warning system—to the fiscal 2003 budget. However, none of the strategies included an analysis of the cost and resources needed to implement the entire strategy. For example, while the cybersecurity R&D strategic plan mentioned specific initiatives, such as a Defense Advanced Research Projects Agency program to fund biologically inspired cyber-attack resilience, it did not describe how decisions were made regarding the amount of resources to be invested in this or any other R&D initiative. The plan also did not outline how the chosen cybersecurity R&D efforts would be funded and sustained in the future.

In addition, the strategies did not include a business case for investing in activities to support their goals and objectives based on assessments of the risks and relative costs of mitigating them. Many of the private sector experts we consulted stated that not establishing such a value proposition makes it difficult to mobilize the resources needed to significantly improve security within the government as well as to build support in the private sector for a national commitment to cybersecurity. A convincing assessment of the specific risks and resources needed to mitigate them would help implementing parties allocate resources and investments according to priorities and constraints, track costs and performance, and shift existing investments and resources as needed to align with national priorities.

Roles and Responsibilities

Most of the strategies lacked clearly defined roles and responsibilities for key agencies, such as DHS, DOD, and OMB, that contribute substantially to the nation's cybersecurity programs. For example, as already discussed, while the law gives OMB responsibility for oversight of federal government information security, OMB transferred several of its oversight responsibilities to DHS. According to OMB representatives, the oversight responsibilities transferred to DHS represent the operational aspects of its role, in contrast to the general oversight responsibilities stipulated by FISMA, which OMB retained. The representatives further stated that the enlistment of DHS to assist OMB in performing these responsibilities has allowed OMB to have more visibility into the cybersecurity activities of federal agencies because of the additional resources and expertise provided by DHS and that OMB and DHS continue to work closely together. While OMB's decision to transfer several of its responsibilities to DHS may have had beneficial practical results, such as leveraging the resources of DHS, it is not consistent with FISMA, which assigns all of these responsibilities to OMB.

With these responsibilities now divided between the two organizations, it is also unclear how OMB and DHS are to share oversight of individual departments and agencies, which are responsible under FISMA for ensuring the security of their information systems and networks. For example, both DHS and OMB have issued annual FISMA reporting instructions to agencies, which could create confusion among agency officials. Further, the instructions vary in content. In its 2012 instructions, DHS included, among other things, specific actions agencies were required to complete, time frames for completing the actions, and reporting metrics. However, the OMB instructions, although identically titled, included different directions. Specifically, the OMB instructions required agencies to submit metrics data for the first quarter of the fiscal year, while the DHS reporting instructions stated that agencies were not required to submit such data. Further, the OMB instructions stated that agency chief information officers would submit monthly data feeds through the FISMA reporting system, while the DHS instructions indicated that inspectors general and senior agency officials for privacy would also submit monthly data feeds. Issuing identically titled reporting instructions with varying content could result in inconsistent reporting.

Further, it is unclear which agency currently has the role of ensuring that agencies are held accountable for implementing the provisions of FISMA. Although FISMA requires OMB to approve or disapprove agencies' information security programs, OMB has not made explicit statements that would indicate whether an agency's information security program has

been approved or disapproved. As a result, a mechanism for establishing accountability and holding agencies accountable for implementing effective programs is not being used.

Mirroring these shortcomings, several GAO reports have likewise demonstrated that the roles and responsibilities of key agencies charged with protecting the nation's cyber assets are inadequately defined. For example, as described in our recent report on gaps in homeland defense and civil support guidance,[43] although DOD has prepared guidance regarding support for civilian agencies in a domestic cyber incident and has an agreement with DHS for preparing for and responding to such incidents, these documents do not clarify all key aspects of how DOD will support a response to a domestic cyber incident. For example, the chartering directives for the Offices of the Assistant Secretary of Defense for Global Strategic Affairs and the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs[44] assign overlapping roles and responsibilities for preparing for and responding to domestic cyber incidents. In an October 2012 report, we recommended that DOD update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance and that such guidance should include a description of DOD's roles and responsibilities. Further, in a March 2010 report on the CNCI,[45] we stated that federal agencies had overlapping and uncoordinated responsibilities and it was unclear where overall responsibility for coordination lay. We recommended that the Director of OMB better define roles and responsibilities for all key CNCI participants to ensure that essential government-wide cybersecurity activities are fully coordinated.

Many of the experts we consulted agreed that the roles and responsibilities of key agencies are not well defined. Clearly defining roles and responsibilities for agencies charged with implementing key aspects

[43]GAO, Homeland Defense: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance, GAO-13-128 (Washington, D.C.: Oct. 24, 2012).

[44]Department of Defense Directive 5111.18, Assistant Secretary of Defense for Global Strategic Affairs (June 13, 2011); and Department of Defense Directive 5111.13, Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (Jan. 16, 2009).

[45]GAO, Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative, GAO-10-338 (Washington, D.C.: Mar. 5, 2010).

of the national cybersecurity strategies would aid in fostering coordination, particularly where there is overlap, and thus enhance both implementation and accountability.

Linkage with Other Key Strategy Documents

The cybersecurity strategy documents we reviewed did not include any discussion of how they linked to or superseded other documents, nor did they describe how they fit into the overall national cybersecurity strategy. For example, the 2003 National Strategy to Secure Cyberspace does not refer to the 2000 plan nor describe progress made since the previous strategy was issued or if it was meant to replace or enhance the previous strategy. Each of the subsequent documents that have addressed aspects of the federal government's approach to cybersecurity—such as the Comprehensive National Cybersecurity Initiative, the National Strategy for Trusted Identities in Cyberspace, and the International Strategy to Secure Cyberspace—has established its own set of goals and priority actions, but none of these cybersecurity agendas are linked to each other to explain why planned activities differ or are prioritized differently. For example, in 2012, the administration determined that trusted Internet connections, continuous monitoring, and strong authentication should be cross-agency priorities, but no explanation was given as to how these three relate to priorities established in other strategy documents. Specifying how new documents are linked with the overall national cybersecurity strategy would clarify priorities and better establish roles and responsibilities, thereby fostering effective implementation and accountability.

The importance of developing an overarching strategy that links component documents and addresses all key elements was confirmed by our discussions with experts. For example, experts agreed that a strategy should define milestones for achieving specific outcomes and that it should be linked to accountability and execution with performance measures to help in determining whether progress is being made. Without addressing these key elements, the national cybersecurity strategy remains poorly defined and faces many implementation challenges. Until an overarching strategy is developed that addresses these elements, progress in cybersecurity may remain limited and difficult to determine.

e r r rPg a t G 7ee3 yeAy-8Gy ui 1g

The Federal Government Continues to Face Challenges in Implementing Cybersecurity that Could Be Addressed by an Effective Strategy

As demonstrated in our reviews and the reviews of inspectors general, the government continues to face cybersecurity implementation challenges in a number of key areas, including those related to protecting our nation's critical infrastructure. For example, audits of federal agencies have found that weaknesses in risk-based management and implementation of controls have not substantially improved over the last 4 years. Incident response capabilities, while becoming more sophisticated, also face persistent challenges in sharing information and developing analytical capability. Challenges likewise remain in developing effective initiatives for promoting education and awareness, coordinating research and development, and interacting with foreign governments and other international entities. Until steps are taken to address these persistent challenges, overall progress in improving the nation's cybersecurity posture is likely to remain limited.

Federal Agencies Face Challenges in Designing and Implementing Risk-based Programs

Developing, implementing, and maintaining security controls is key to preventing successful attacks on computer systems and ensuring that information and systems are not compromised. Ineffective implementation of security controls can result in significant risks, including

- loss or theft of resources, including money and intellectual property;
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- use of computer resources for unauthorized purposes or to launch attacks on other computer systems;
- damage to networks and equipment;
- loss of business due to lack of customer confidence; and
- increased costs from remediation.

From a strategic perspective, it is important that effective processes be instituted for determining which controls to apply, ensuring they are properly implemented, and measuring their effectiveness. Such processes are core elements of an effective cybersecurity strategy.

Federal Strategies and Guidance Reflect a Risk-based Approach

Federal strategy documents reflect the risk-based approach to managing information security controls established by FISMA and federal guidance. For example, the 2003 National Strategy to Secure Cyberspace

recognizes the importance of managing risk responsibly and enhancing the nation's ability to minimize the damage that results from successful attacks. It encourages the use of commercially available automated auditing and reporting tools to validate the effectiveness of security controls, and states that these tools are essential to continuously understanding the risks to information systems. While acknowledging the importance of these principles, the 2003 strategy document did not indicate time frames or milestones for accomplishing specific actions or establish measures to determine the progress in achieving those actions.

The 2009 White House Cyberspace Policy Review provided more specifics, stating that the federal government, along with state, local, and tribal governments and industry, should develop a set of threat scenarios and metrics that all could use for risk management decisions. The DHS Blueprint for a Secure Cyber Future,[46] released in November 2011, included reducing exposure to cyber risk as one of its four goals for protecting critical information infrastructure. According to the blueprint, to achieve this goal the department must identify and harden critical information infrastructure through the deployment of appropriate security measures to manage risk to critical systems and assets.

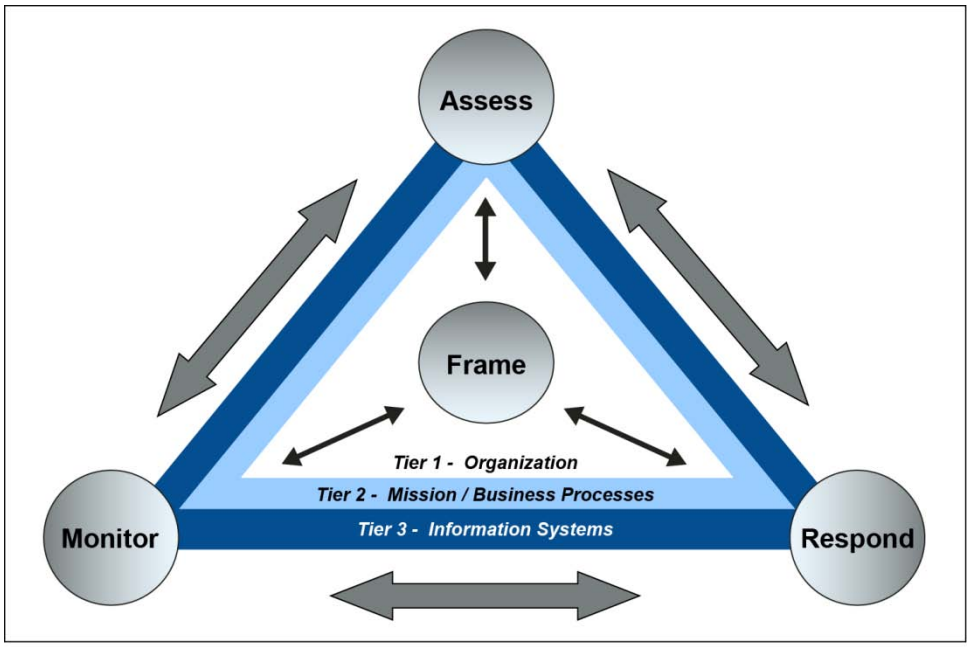
As discussed previously, OMB, in July 2010, issued a memorandum expanding DHS's cybersecurity role in overseeing federal agencies' implementation of FISMA requirements. As part of DHS's responsibilities for FISMA reporting, the Cybersecurity Performance Management Program within DHS annually reviews FISMA data submitted by agencies and inspectors general to, among other things, identify cyber risks across the federal enterprise. This information informs the annual report to Congress.

To assist agencies in identifying risks, NIST has released risk management and assessment guides for information systems.[47] These

[46]DHS issued the Blueprint for a Secure Cyber Future to establish a plan of action for the department to implement the National Security Strategy and to achieve other DHS cybersecurity goals.

[47]NIST, Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39 (Gaithersburg, Md.: March 2011); Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37 Revision 1 (Gaithersburg, Md.: February 2010); and Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

guides provide a foundation for the development of an effective risk management program, and include the guidance necessary for assessing and mitigating risks identified within information technology systems. Agencies are required to use these guidance documents when identifying risks to their systems. NIST's guide for managing information security risk provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations, organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems. The guide describes fundamental concepts associated with managing information security risk across an organization, including risk management at various levels, called tiers. According to NIST, risk management is a process that requires organizations to (1) frame risk (i.e., establish the context for risk-based decisions); (2) assess risk; (3) respond to risk once determined; and (4) monitor risk on an ongoing basis. Figure 4 illustrates the risk management process as applied across the tiers—organization, mission/business process, and information system.



Source: NIST data.

Shortcomings Persist in Assessing Risk, Developing and Implementing Controls, and Monitoring Results in the Federal Government

Our audits and the audits of inspectors general have identified many weaknesses in agencies' risk management processes. Numerous recommendations were made to agencies in fiscal years 2011 and 2012 to address these security control weaknesses, which include risk assessment weaknesses, inconsistent application of controls, and weak monitoring controls.

Assessing Risk

According to NIST, risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. These assessments increase an organization's awareness of risk and can generate support for policies and controls that are adopted in response. Such support can help ensure that policies and controls operate as intended. In addition, identifying and assessing information security risks are essential to determining what controls are required.

Agencies' capabilities for performing risk assessments, as required by FISMA, have declined in recent years. According to OMB's fiscal year 2011 report to Congress on FISMA implementation, agency compliance with risk management requirements suffered the largest decline of any FISMA metric between fiscal year 2010 and 2011. Inspectors general for 8 of 22 major agencies reported compliance in 2011, while 13 of 24 inspectors general reported compliance the year before. The following deficiencies were cited most frequently:

- accreditation boundaries for agency systems were not defined (13 of 23 agencies),
- specific risks were not sufficiently communicated to appropriate levels of the organization (12 of 23 agencies),
- risks from a mission or business process perspective were not addressed (12 of 23 agencies), and
- security assessment report was not in accordance with government policies (11 of 23 agencies).

Our own analysis of weaknesses reported by inspectors general shows that the number of weaknesses related to the risk assessment process

has greatly increased over the last 4 years. In fiscal year 2008 only 3 of the 24 inspectors general reported weaknesses related to assessing risk. In fiscal year 2011, 18 of 24 reported weaknesses in this area. For example, according to a November 2011 inspector general report, one agency did not have a risk management framework in place and had not fully developed risk management procedures, due to budget cuts. Around the same time, another agency's inspector general reported that while risk management procedures at a system-specific level had been implemented, an agency-wide risk management methodology had not been developed. In an October 2011 report on agencies' efforts to implement information security requirements, we reported that of the 24 major agencies, none had fully or effectively implemented an agency-wide information security program.[48] Of those, 18 had shortcomings in the documentation of their security management programs, which establish the framework and activities for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

Risk management was also a topic that our experts felt was very important to a comprehensive approach to cybersecurity. One expert stated that cybersecurity is not a technical problem, but an enterprise-wide risk management challenge that must be tackled in a far more comprehensive manner than is generally understood both at the enterprise and government level. One expert cited defining the cost of insecurity as one of the most significant challenges in improving the nation's cybersecurity posture. Another expert suggested that the risk guidance be reviewed and updated due to changes in technology.

Developing and Implementing Appropriate Controls

NIST has developed guidance to assist agencies, once risks have been assessed, in determining which controls are appropriate for their information and systems. In August 2009, NIST released the third revision of special publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, which provides a catalog of controls and technical guidelines that federal agencies must use to

[48]GAO, Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements, GAO-12-137 (Washington, D.C.: Oct. 3, 2011).

protect federal information and information systems.[49] The use of this NIST guidance for nonfederal information systems, such as those in the nation's critical infrastructure, is encouraged but not required.

Agencies have flexibility in applying NIST guidance, and according to NIST, agencies should apply the security concepts and principles articulated in special publication 800-53 in the context of the agency's missions, business functions, and environment of operation.

In addition, in order to ensure a consistent government-wide baseline, specific guidance has been developed for implementing and configuring controls in certain widely used computing platforms. In fiscal year 2010, DOD, DHS, NIST, and the federal CIO Council worked closely together to develop the United States Government Configuration Baseline (USGCB) for Windows 7 and Internet Explorer 8. As a baseline, USGCB is the core set of default security configurations for all agencies; however, agencies may customize the USGCB baseline to fit their operational needs. In fiscal year 2011, the USGCB was expanded to include RedHat Enterprise Linux 5 Desktop, and multiple updates for Windows 7 and Internet Explorer 8 were released.

Although guidance for implementing appropriate cybersecurity controls has been available for many years, we have consistently identified weaknesses in agencies' implementation of the guidance in control areas such as configuration management. Configuration management is an important process for establishing and maintaining secure information system configurations, and provides important support for managing security risks in information systems. However, inspectors general have consistently reported weaknesses in agencies' implementation of such controls. For example, the fiscal year 2011 report to Congress on the implementation of FISMA listed configuration management as one of the 11 cybersecurity program areas[50] that needed the most improvement. According to that report, 18 of 24 agencies' configuration management

[49]NIST released an update of this publication in May 2010. An initial public draft for comment of the fourth revision of this publication was released in February 2012.

[50]Each inspector general is asked to assess his or her agency's information security programs in 11 areas: risk management, configuration management, incident response and reporting, security training, plans of actions and milestones, remote access management, identity and access management, continuous monitoring management, contingency planning, contractor systems, and security capital planning.

programs needed significant improvement. The following deficiencies were found to be the most common:

- configuration management policy was not fully developed (13 of 23 agencies),
- configuration management procedures were not fully developed (9 of 23 agencies),
- standard baseline configurations were not identified for all hardware components (9 of 23 agencies), and
- USGCB was not fully implemented (8 of 23 agencies).

Our own analysis of weaknesses reported by agency inspectors general also shows that the number of weaknesses related to configuration management has increased over the last 4 years. In fiscal year 2008, inspectors general from 15 agencies reported weaknesses related to configuration management, whereas 23 reported weaknesses in 2011.

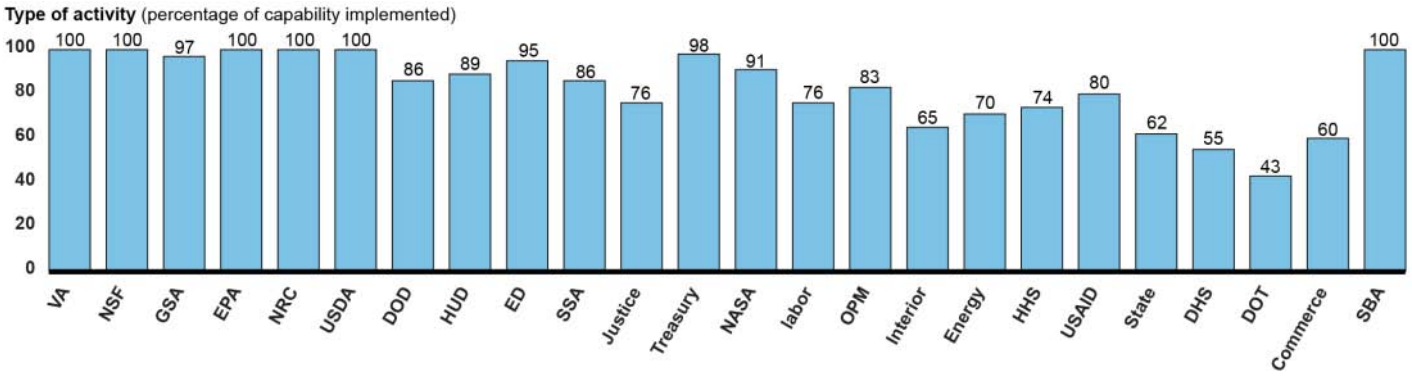
The experts we consulted focused on the need for security controls to be included in systems development, instead of being applied as an afterthought. One expert stated that commercial companies often forgo the extra cost associated with meeting defined cybersecurity specifications, and security is weakened as a result of the lack of built-in controls. Another expert made a similar comment by saying that one of the most significant changes that would improve cybersecurity is building in security instead of "bolting it on" after the fact. He added that this would involve changing the mindset of various stakeholders.

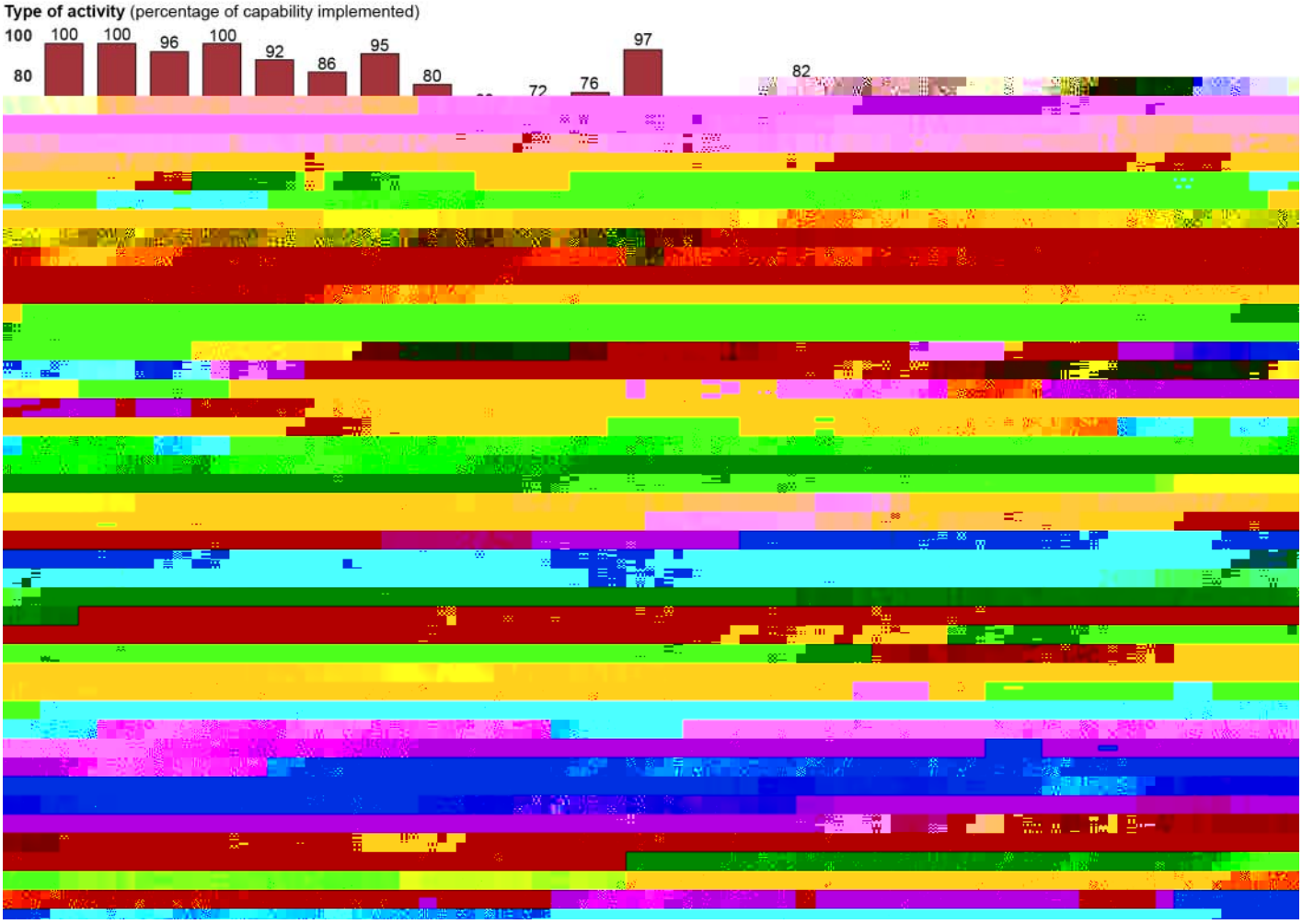
Monitoring Results

According to NIST, security control effectiveness is measured by correctness of implementation and by how adequately the implemented controls meet organizational needs in accordance with current risk tolerance (i.e., whether the control is implemented in accordance with the security plan to address threats and whether the security plan is adequate). Further, according to NIST, a key element in implementing an effective risk management approach is to establish a continuous monitoring program. Continuous monitoring is the process of maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objectives are to (1) conduct ongoing monitoring of the security of an organization's

networks, information, and systems; and (2) respond by accepting, transferring, or mitigating risk as situations change. Continuous monitoring is one of the six steps in NIST's risk management framework and is an important way to assess the security impacts on an information system due to changes in hardware, software, firmware, or environmental operations. As part of its reporting instructions since fiscal year 2010, OMB requested inspectors general to report whether agencies had established continuous monitoring programs. For fiscal year 2011, the administration identified continuous monitoring as one of three FISMA priorities, and therefore the fiscal year 2011 FISMA reporting instructions included expanded metrics related to continuous monitoring.

OMB's fiscal year 2011 report on the implementation of FISMA shows that, according to agency reporting, implementation of automated continuous monitoring capabilities rose from 56 percent of total assets in fiscal year 2010 to 78 percent of total assets in fiscal year 2011. Agencies reported that they had implemented automated capabilities for activities such as inventorying assets, configuration management, and vulnerability management, which contributed to improvements in continuous monitoring capabilities (see fig. 5).


Type of activity (percentage of capability implemented)
100
80
60
40
20
0
100 100 97 100 100 100 86 89 95 86 76 98 91 76 83 65 70 74 80 62 55 43 60 100
VA NSF GSA EPA NRC USDA DOD HUD ED SSA Justice Treasury NASA labor OPM Interior Energy HHS USAID State DHS DOT Commerce SBA


Type of activity (percentage of capability implemented)
100
80
100 100 96 100 92 86 95 80 72 76 97 82

sources.[5] We also selected the last two White House cybersecurity advisors.

Lastly, we reviewed agency inspector general and GAO reports that previously identified challenges related to government-wide cybersecurity strategies and initiatives, and met with staff from the DHS Office of Inspector General to determine the current status of related recommendations in their prior reports. We then assessed progress in overcoming the inspector general- and GAO-identified challenges through interviews with agency officials and reviewing agency documentation and publicly available data.

We performed our work on the initiative of the U.S. Comptroller General to evaluate the federal government's cybersecurity strategies and understand the status of federal cybersecurity efforts to address challenges in establishing a strategic cybersecurity approach.

We conducted this performance audit from April 2012 to February 2013 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.

[5]Being listed as a member of the Computer Science and Telecommunications Board and one or more of its committees was counted as a single source. Similarly, testifying at multiple congressional hearings also counted as a single source.

Appendix II: List of Panel and Survey Participants

This appendix lists the names and affiliations of the cybersecurity and information management professionals who participated in the cybersecurity expert panel discussion and the Executive Committee for Information Management and Technology panel discussion, as well as the respondents to our surveys of cybersecurity experts and agency CIOs.

Cybersecurity Expert Panel Discussion Attendees

The names and affiliation of the cybersecurity experts, who participated in the panel held September 14, 2012, in Washington D.C., are as follows:

Stewart A. Baker, Partner, Steptoe & Johnson LLP

Steven M. Bellovin, Professor of Computer Science at Columbia University

Dan Chenok, Executive Director, IBM Center for The Business of Government; Chair of NIST's Information Security and Privacy Advisory Board

Larry Clinton, President and CEO, Internet Security Alliance

Tom Gann, Vice President of Government Relations, McAfee

Seymour E. Goodman, Professor of International Affairs and Computing, Sam Nunn School of International Affairs, College of Computing at Georgia Institute of Technology

Susan Landau, Independent Scholar

Herbert Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies

Randy V. Sabett, Counsel, ZwillGen LLP

Howard Schmidt, former Cybersecurity Coordinator, Executive Office of the President of the United States; Special Assistant, President of the United States

Executive Committee for Information Management and Technology Panel Discussion Attendees

The names and affiliation of the experts who participated in the panel discussion held September 12, 2012, in Washington D.C., are as follows:

Lynda Applegate, Harvard Business School

Hank Conrad, CounterPoint Corporation

Mary Culnan, Bentley University

John Flynn, Principal, FK&A Inc.

Peter Neumann, SRI International Computer Science Laboratory

Theresa Pardo, Director, Center for Technology in Government, University at Albany, New York

Douglas Robinson, Executive Director, National Association of State Chief Information Officers (NASCIO)

Paul Rummell, Management Consultant

Dugan Petty, State of Oregon and NASCIO

Eugene H. Spafford, CERIAS, Purdue University

Nancy Stewart, Wal-Mart (retired)

Aldona Valicenti, VP Government Markets, CGI

James B. Whittaker, Whittaker Group

John A. Zachman, President, Zachman International

Expert and CIO Survey Participants

Expert Survey Participants

Stewart A. Baker, Partner, Steptoe & Johnson LLP

Steven M. Bellovin, Professor of Computer Science at Columbia University

Scott Borg, Director and Chief Economist, United States Cyber Consequence Unit

Dan Chenok, Executive Director, IBM Center for the Business of Government; Chair of NIST's Information Security and Privacy Advisory Board

Larry Clinton, President and CEO, Internet Security Alliance

Tom Gann, Vice President of Government Relations, McAfee

Seymour E. Goodman, Professor of International Affairs and Computing, Sam Nunn School of International Affairs, College of Computing at Georgia Institute of Technology

Susan Landau, Independent Scholar

James Lewis, Director and Senior Fellow of Technology and Public Policy, Center for Strategic and International Studies

Herbert Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies

Randy V. Sabett, Counsel, ZwillGen LLP

Peter Weinberger, Senior Software Engineer, Google

CIO Survey Participants

Darren B. Ash, U.S. Nuclear Regulatory Commission

Frank Baitman, Department of Health and Human Services

Roger W. Baker, Department of Veterans Affairs

Danny A. Harris, Department of Education

Bernard J. Mazer, Department of the Interior

Matthew E. Perry, Office of Personnel Management

Tim Schmidt, Department of Transportation

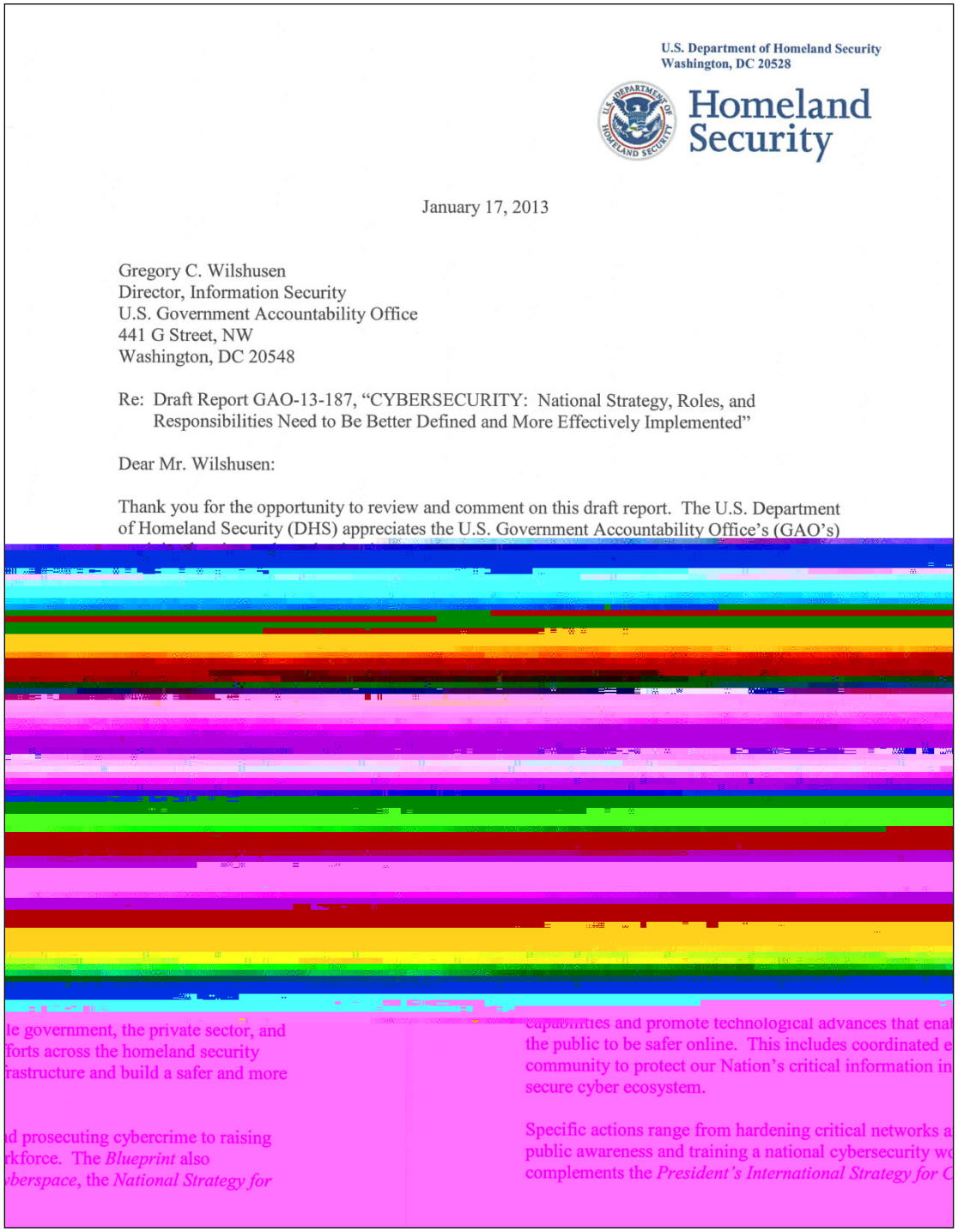
Richard Spires, Department of Homeland Security

Simon Szykman, Department of Commerce

Steven C. Taylor, Department of State

Eric Won, Small Business Administration

Appendix III: Comments from the Department of Homeland Security



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

Homeland Security

January 17, 2013

Gregory C. Wilshusen
Director, Information Security
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

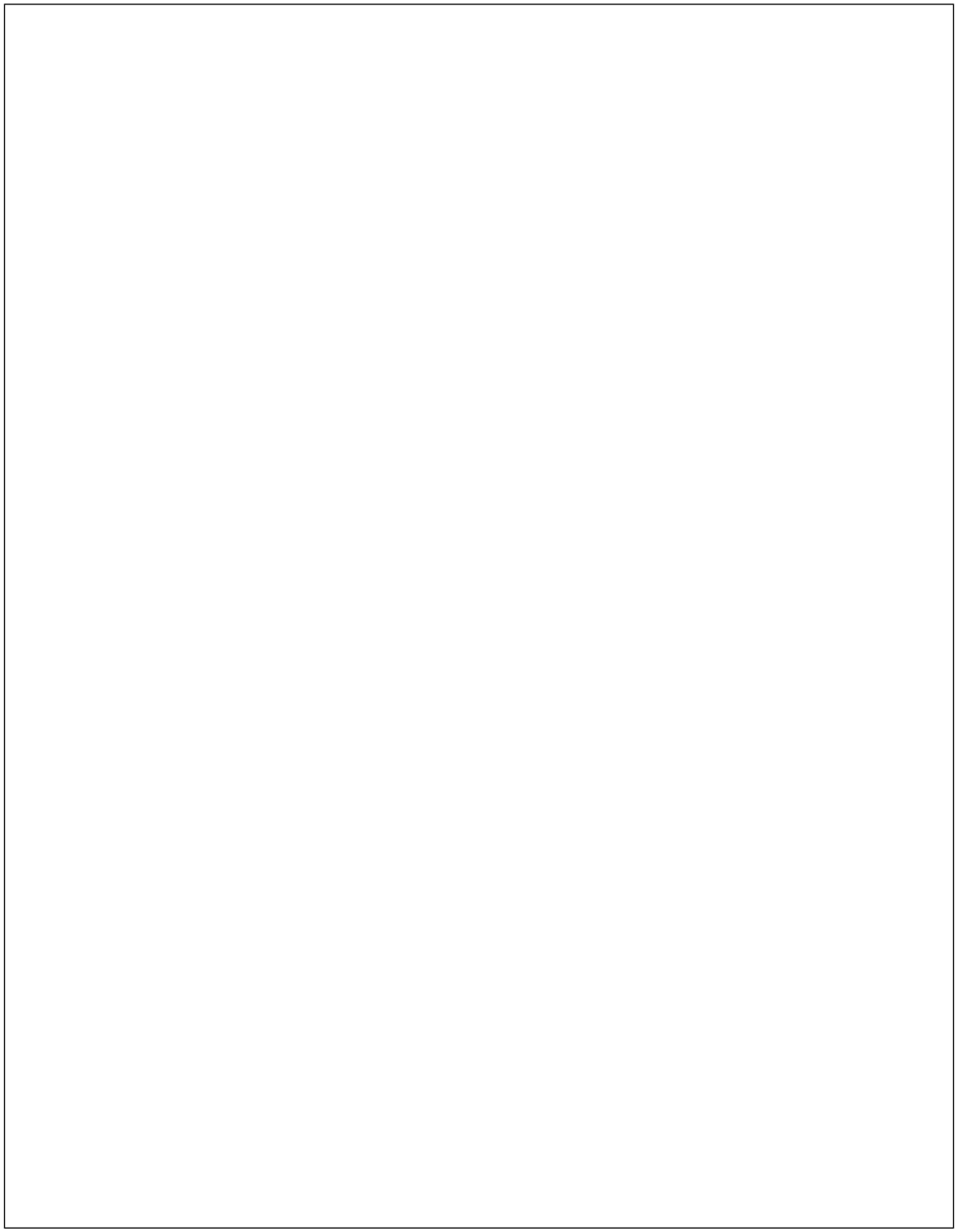
Re: Draft Report GAO-13-187, "CYBERSECURITY: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's)

le government, the private sector, and
forts across the homeland security
rastructure and build a safer and more

d prosecuting cybercrime to raising
rkforce. The *Blueprint* also
berspace, the *National Strategy for*

capabilities and promote technological advances that enat
the public to be safer online. This includes coordinated e
community to protect our Nation's critical information in
secure cyber ecosystem.

Specific actions range from hardening critical networks a
public awareness and training a national cybersecurity wo
complements the *President's International Strategy for C*