United States Government Accountability Office

GAO

Report to Congressional Requesters

December 2011

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use

GAO-12-92

December 2011

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-92, a report to congressional requesters

Why GAO Did This Study

Critical infrastructures are systems and assets critical to the nation's security, economy, and public health and safety, most of which are owned by the private sector. These assets rely on networked computers and systems, thus making them susceptible to cyber-based risks. Managing such risk involves the use of cybersecurity guidance that promotes or requires actions to enhance the confidentiality, integrity, and availability of computer systems.

For seven critical infrastructure sectors, GAO was asked to identify (1) cybersecurity guidance for entities within the sectors, (2) the extent to which implementation of this guidance is enforced and promoted, and (3) areas of commonalities and differences between sector cybersecurity guidance and guidance applicable to federal agencies. To do this, GAO collected and analyzed information from responsible private sector coordinating councils; federal agencies, including sector-specific agencies that are responsible for coordinating critical infrastructure protection efforts; and standards-making bodies. In addition, GAO compared a set of guidance in each of three subsectors with guidance applicable to federal agencies.

What GAO Recommends

GAO is recommending that the Department of Homeland Security (DHS), in collaboration with public and private sector partners, determine whether it is appropriate to have cybersecurity guidance listed in sector plans. DHS concurred with GAO's recommendation.

View GAO-12-92. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

A wide variety of cybersecurity guidance is available from national and international organizations for entities within the seven critical infrastructure sectors GAO reviewed—banking and finance; communications; energy; health care and public health; information technology; nuclear reactors, material, and waste; and water. Much of this guidance is tailored to business needs of entities or provides methods to address unique risks or operations. In addition, entities operating in regulated environments are subject to mandatory standards to meet their regulatory requirements; entities operating outside of a regulatory environment may voluntarily adopt standards and guidance. While private sector coordinating council representatives confirmed lists of cybersecurity guidance that they stated were used within their respective sectors, the representatives emphasized that the lists were not comprehensive and that additional standards and guidance are likely used.

Implementation of cybersecurity guidance can occur through a variety of mechanisms, including enforcement of regulations and voluntarily in response to business incentives; however, sector-specific agencies could take additional steps to promote the most applicable and effective guidance throughout the sectors. A number of subsectors within the sectors included in GAO's review, such as electricity in the energy sector, are required to meet mandatory cybersecurity standards established by regulation under federal law or face enforcement mechanisms, such as civil monetary penalties. By contrast, entities not subject to regulation may voluntarily implement cybersecurity guidance to, among other things, reduce risk, protect intellectual property, and meet customer expectations. Federal policy establishes the dissemination and promotion of cybersecurity-related standards and guidance as a goal to enhancing the security of our nation's cyber-reliant critical infrastructure. DHS and the other lead agencies for the sectors selected for review have disseminated and promoted cybersecurity guidance among and within sectors. However, DHS and the other sector-specific agencies have not identified the key cybersecurity guidance applicable to or widely used in each of their respective critical infrastructure sectors. In addition, most of the sector-specific critical infrastructure protection plans for the sectors reviewed do not identify key guidance and standards for cybersecurity because doing so was not specifically suggested by DHS guidance. Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.

Sector cybersecurity guidance that GAO compared in three subsectors within the banking and finance, energy, and nuclear sectors is substantially similar to guidance applicable to federal agencies. Specifically, one set of guidance for each subsector, along with supplementary documents, addressed most risk management steps and most recommended security controls that are specified for federal information systems in guidance from the Commerce Department's National Institute of Standards and Technology.

Contents

Abbreviations

ANSI	American National Standards Institute
CIP	critical infrastructure protection
DHS	Department of Homeland Security
FERC	Federal Energy Regulatory Commission
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Management Act
HHS	Department of Health and Human Services
HSPD-7	Homeland Security Presidential Directive 7
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	information technology
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCR	Office for Civil Rights
SCC	sector coordinating council
SP	special publication

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

December 9, 2011

Congressional Requesters

Federal policy identifies infrastructure sectors—such as banking and finance, energy, health care and public health, and communications—that are critical to the nation's security, economy, and public health and safety.[1] Because these sectors rely extensively on computerized information systems and electronic data, the effective implementation of appropriate security over these systems and data is crucial. Further, because most of these infrastructures are privately owned, it is imperative that public and private entities work together to protect these assets. Since 2003 we have identified protecting systems supporting our nation's critical infrastructure—referred to as cyber-critical infrastructure protection, or cyber CIP—as a governmentwide high-risk area, and we continue to do so in the most recent update to our high-risk list.[2]

To better manage cyber-based risks, public and private organizations use cybersecurity guidance that promotes or requires action to enhance the confidentiality, integrity, and availability of computer systems.[3] In addition, for certain entities, such as financial institutions and nuclear power plants, federal laws, regulations, and mandatory guidance require actions to enhance the security of their information technology (IT) systems and data.

[1]Federal policy established 18 critical infrastructure sectors: banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; food and agriculture; government facilities; health care and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water.

[2]GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure. See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[3]As used in this report, cybersecurity guidance includes voluntary, consensus-based standards and mandatory or required standards, implementation guides and manuals, and best or smart practices.

As agreed, our objectives were to identify (1) cybersecurity guidance for entities within selected critical infrastructure sectors, (2) the extent to which implementation of cybersecurity guidance is enforced and promoted within selected sectors, and (3) areas of commonalities and differences that exist between sectors' cybersecurity guidance and guidance applicable to federal agencies. To accomplish these objectives, we focused our efforts on seven sectors and certain subsectors: banking and finance; communications; energy (electricity and oil and natural gas); health care and public health; information technology; nuclear reactors, materials, and waste; and water. We collected and analyzed information from the federal agencies responsible for overseeing each critical infrastructure sector—referred to as sector-specific agencies—private councils established to coordinate critical infrastructure protection policy—referred to as sector coordinating councils (SCC)—and other sources to identify cybersecurity guidance, efforts to promote cybersecurity guidance within the sectors, and mechanisms and authorities available to enforce compliance with the mandatory guidance. In addition, we compared the cybersecurity guidance available to a subsector within each of three sectors (banking and finance, energy, and nuclear) with federal cybersecurity guidance to identify areas of commonalities and differences. Further details of our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from October 2010 to December 2011 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.

Background

Critical infrastructures are systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on national security, economic well-being, public health or safety, or any combination of these. Critical infrastructure includes, among other things, banking and financial institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned by the private sector. As these critical infrastructures have become increasingly dependent on computer systems and networks, the interconnectivity among information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt critical systems, with potentially harmful effects. To better

manage cyber-based risks that the nation's cyber-reliant critical infrastructure faces, public and private organizations use available cybersecurity standards and guidance that promote the security of their critical systems.

Cyber-Reliant Critical Infrastructures Face a Proliferation of Threats

Threats to systems supporting critical infrastructure are evolving and growing. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[4] Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

These cyber threat sources can use various cyber exploits that may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself. Groups or individuals may intentionally deploy cyber exploits targeting a specific cyber asset or indiscriminately attack through the Internet using a virus, worm, or malware with no specific target. The potential impact of these threats is amplified by the connectivity among information systems, the Internet, and other infrastructures, creating opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. For example, in May 2008, we reported that the Tennessee Valley Authority's corporate network contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[5] Accordingly, we made several recommendations to address these weaknesses. Tennessee Valley Authority officials concurred with the recommendations and have since taken steps to resolve these weaknesses. As government, private sector, and personal activities

[4]Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community, statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

[5]GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

continue to move to networked operations, the threat will continue to grow. Table 1 provides descriptions of common types of cyber exploits.

Table 1: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run 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 bomb	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.
SQL 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 computer 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 computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed time frame between public discoveries of both makes it difficult to defend against.

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

Reports of cyber attacks illustrate that such attacks could have a debilitating impact on national and economic security and on public health and safety.

- In June 2011, a major bank reported that hackers had broken into its systems and gained access to the personal information of hundreds of

thousands of customers. Through the bank's online banking system, the attackers were able to view certain private customer information.
- In February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- In July 2010, a sophisticated computer attack, known as Stuxnet, was discovered. It targeted control systems used to operate industrial processes in the energy, nuclear, and other critical sectors. It is designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.

Federal Law and Policy Emphasizes Public-Private Coordination and the Provision of Guidance for the Protection of Cyber-Reliant Critical Assets

Federal law and policy have established roles and responsibilities for federal agencies working with the private sector and other entities in enhancing the cyber and physical security of critical public and private infrastructures. These include the Homeland Security Act of 2002,[6] Homeland Security Presidential Directive 7 (HSPD-7),[7] and the National Infrastructure Protection Plan (NIPP).[8] In addition, regulatory entities oversee entities within critical infrastructure sectors and develop and publish various types of cybersecurity guidance to assist their examiners and organizations.

The Homeland Security Act of 2002 created the Department of Homeland Security (DHS). Among other things, it assigned the department the following critical infrastructure protection responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States; (2) assisting in the development and promotion of private sector best practices to secure critical infrastructure; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of, or response to, terrorist attacks.

HSPD-7 established DHS as the principal federal agency to lead, integrate, and coordinate the implementation of efforts to protect cyber-

[6]Homeland Security Act of 2002, Pub. L. No. 107-296 (Nov. 25, 2002).

[7]The White House, Homeland Security Presidential Directive 7 (Washington, D.C.: December 2003).

[8]Department of Homeland Security, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (2009).

critical infrastructures and key resources. In addition, HSPD-7 identified lead federal agencies, referred to as sector-specific agencies, which are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors. For example, the Department of the Treasury and the Department of Health and Human Services are the sector-specific agencies for the banking and finance and the health care and public health sectors, respectively.

The NIPP states that, in accordance with HSPD-7, DHS is a principal focal point for the security of cyberspace and is responsible for coordinating efforts to protect the cyber infrastructure to ensure its confidentiality, integrity, and availability. These responsibilities, among other things, include providing guidance on effective cyber-protective measures, assisting the sector-specific agencies in understanding and mitigating cyber risk, and assisting in developing effective and appropriate protective measures. To accomplish these responsibilities, DHS is to help in the development of comprehensive cybersecurity guidance that homeland security partners may adopt to meet accepted industry-based standards that measurably reduce the risk of cyber disruption or exploitation.

The NIPP also describes a partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure. For each sector, the model requires formation of government coordinating councils—composed of federal, state, local, or tribal agencies with purview over critical sectors—and encourages voluntary formation of SCCs—composed of owner-operators of these critical assets (some of which may be state or local agencies) or their respective trade associations. These councils create the structure through which representative groups from all levels of government and the private sector are to collaborate in planning and implementing efforts to protect critical infrastructure. The sector councils are envisioned to be policy-related and to represent a primary point of contact for government to plan the entire range of infrastructure protection activities, including those associated with mitigating cyber threats.

According to the NIPP, sector-specific agencies are to work with their private sector counterparts to understand and mitigate cyber risk by, among other things, determining whether approaches for critical infrastructure inventory, risk assessment, and protective measures address assets, systems, and networks; require enhancement; or require the use of alternative approaches. They are also to review and modify existing and future sector efforts to ensure that cyber concerns are fully

integrated into sector security activities and protective activities. Table 2 shows the 18 critical infrastructure sectors and the sector-specific agencies assigned to each sector.

Table 2: Critical Infrastructure Sectors and Sector-Specific Agencies

Critical infrastructure sector	Description	Sector-specific agencies
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.	Department of the Treasury
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	DHS
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	DHS
Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS
Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.	DHS
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	DHS
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	DHS
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food and agriculture	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	Department of Agriculture Department of Health and Human Services (Food and Drug Administration)
Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.	DHS
Health care and public health	Protects the health of the population before, during, and after disasters and attacks. The sector consists of direct health care, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.	Department of Health and Human Services

Critical infrastructure sector	Description	Sector-specific agencies
Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS
National monuments and icons	Maintains monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.	Department of the Interior
Nuclear reactors, materials, and waste	Provides nuclear power. The sector includes commercial nuclear reactors and nonpower nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.	DHS
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	DHS
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	DHS
Water	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.	Environmental Protection Agency

Source: GAO reports and the National Infrastructure Protection Plan.

Further, the NIPP called for the sector-specific agencies, in close collaboration with the sector coordinating councils, government coordinating councils, and others, including state, local, and tribal critical infrastructure key resources partners, to develop sector-specific plans and sector annual reports to address how the sectors would implement the national plan, including how the security of cyber and other (physical) assets and functions was to be improved. More specifically, according to the NIPP,

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

In September 2009, we reported that sector-specific agencies had made limited progress in updating their sector-specific plans to fully address key

cyber elements.[9] As a result, we recommended that the Secretary of Homeland Security, consistent with any direction from the Office of the Cybersecurity Coordinator,[10] (1) assess whether the existing sector-specific planning process should continue to be the nation's approach to securing cyber and other critical infrastructure and, in doing so, consider whether proposed and other options would provide more effective results and (2) if the existing approach is deemed to be the national approach, work with the sector-specific agencies to develop their plans to fully address DHS cybersecurity criteria. In response to our recommendations, DHS took steps to make sector-specific planning a priority. For example, in 2009 and 2010, DHS met and worked with the sector-specific agencies and sector representatives to update sector plans with the goal of fully addressing cyber-related criteria. As of October 2011, of the 18 plans, DHS reported that 17 have been finalized and approved and 1 is still in the process of being reviewed.

In addition, DHS's *Quadrennial Homeland Security Review Report* identified key strategic outcomes for the department's safeguarding and securing cyberspace mission, including, among others, that the (1) homeland security partners develop, update, and implement guidelines, regulations, and standards that ensure the confidentiality, integrity, and reliability of systems, networks, and data, and (2) critical infrastructure sectors adopt and sector partners meet accepted standards that measurably reduce the risk of cyber disruption or exploitation.[11]

In addition to public-private partnership-related efforts, regulatory entities oversee entities within critical infrastructure sectors that are under the purview of federal law, regulation, or mandatory standards pertaining to

[9]GAO, *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment,* GAO-09-969 (Washington, D.C.: Sept. 24, 2009).

[10]In May 2009, the White House released "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." Among other things, the review recommended appointing of an official in the White House to coordinate the nation's cybersecurity. In December 2009, the President appointed a Special Assistant to the President and Cybersecurity Coordinator to fulfill this role.

[11]DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010).

securing privately owned information systems or data.[12] For example, depository financial institutions (such as commercial banks and credit unions) in the banking and finance sector are regulated by members of the Federal Financial Institutions Examination Council (FFIEC).[13] The mechanisms used to perform oversight include continuous examinations, periodic examinations, self-reporting, and compliance reviews, and various types of mechanisms exist to enforce compliance. Federal regulators also develop and publish various types of cybersecurity guidance to assist (1) the examiners and inspectors in carrying out their responsibilities and (2) the regulated entities in fulfilling requirements, addressing specific threats, or mitigating identified risks. For example, FFIEC has issued handbooks that are intended to provide guidance to examiners and organizations.

Many Organizations Develop Cybersecurity Guidance to Help Manage Cyber-Based Risks

Cybersecurity guidance provides general guidelines and principles as well as technical security techniques for maintaining the confidentiality, integrity, and availability of information systems and data. When implementing cybersecurity technologies and processes, organizations can avoid making common implementation mistakes by consulting guidance developed by various other organizations. Public and private organizations may decide to voluntarily adopt this guidance to help them manage cyber-based risks. Some entities may also be required to meet regulations or mandatory requirements that address cybersecurity.

[12]Federal laws are defined as statutes enacted by the Congress of the United States that pertain to matters that are within the legislative authority delegated to the national government by the United States Constitution. Federal regulations are defined as the general and permanent rules published in the *Federal Register* by a federal department or agency. Federal mandatory standards are defined as requirements adopted by a federal department or agency with the legal authority to regulate the entities or activities that are the subject of the standards. See GAO*, Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors*, GAO-08-1075R (Washington, D.C.: Sept. 16, 2008).

[13]FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. Its membership includes leadership from the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee. The Office of Thrift Supervision, a past member, was dissolved in July 2011, and many of its functions were transferred to the Office of the Comptroller of the Currency.

Many organizations exist that develop standards and guidance that, among other things, promote the confidentiality, integrity, and availability of computer systems and information. Examples of such organizations include the following:

- International Organization for Standardization (ISO): a nongovernmental organization that develops and publishes international standards. The standards, among other things, address information security by establishing guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

- International Electrotechnical Commission (IEC): an organization for standardization comprising all national eletrotechnical committees. The commission publishes international standards, technical specifications, technical reports, and publicly available specifications and guides. The information security standards address safety, security, and reliability in the design and operations of systems in the power industry, among other things.

- The International Telecommunication Union: a United Nations agency whose mission includes, among other things, developing technical standards and providing technical assistance and capacity building to developing countries. The union has also developed technical standards for security and, more recently, engaged in other cybersecurity activities. For example, the union has established a study group for telecommunications security to focus on developing standards and recommendations associated with network and information security, application security, and identity management. Similarly, the union, through its members' efforts, prepared a report on cybersecurity best practices for countries seeking to organize national cybersecurity efforts.

- The International Society of Automation (ISA): a global and nonprofit organization that develops standards for automation. It has developed a series of standards to address security in industrial automation and control systems.

- The American National Standards Institute (ANSI): a U.S. organization that is responsible for coordinating and promoting voluntary consensus-based standards and information sharing to minimize overlap and duplication of U.S. standards-related efforts.

In addition, it is the representative of U.S. interests in international standards-developing organizations.[14]

Individual industries and sectors also have their own specific standards. These include standards or guidance developed by regulatory agencies that assist entities within sectors in complying with cybersecurity-related laws and regulations. In addition, organizations that operate in a specific industry develop cybersecurity standards and guidance and promote practices for their industries.

In the United States, the National Institute of Standards and Technology (NIST), a standards-setting agency under the U.S. Department of Commerce, issues Federal Information Processing Standards that, pursuant to the Federal Information Security Management Act of 2002 (FISMA), are mandatory for federal agencies and special publications that provide guidance for information systems security for non-national security systems.[15] For example, NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* provides guidance for an integrated, organizationwide 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.[16] NIST also developed a risk management framework that is one of several NIST guidelines for federal agencies to follow in developing information security programs. The framework is specified in NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* which provides agencies with guidance for applying the

[14]A December 2000 memorandum of understanding between ANSI and the National Institute of Standards and Technology establishes the organizations' agreement on a unified national approach to developing national and international standards. The memorandum states that ANSI is the representative of U.S. interests in international standards-developing organizations.

[15]FISMA requires that federal agencies comply with NIST information security standards, and agencies may not waive their use. In addition, FISMA emphasizes the need for agencies to develop, document, and implement agencywide programs to provide security for the information systems that support their operations and assets.

[16]NIST, *Managing Information Security Risk, Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

risk management framework to federal information systems.[17] The framework consists of a six-step process involving (1) security categorization, (2) security control selection, (3) security control implementation, (4) security control assessment, (5) information system authorization, and (6) security control monitoring. It also provides a process that integrates information security and risk management activities into the system development life cycle.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* provides a catalog of security controls and technical guidelines that federal agencies use to protect federal information and information systems.[18] Nonfederal entities, such as those in the nation's critical infrastructure sectors, are encouraged but not required to use this NIST guidance where appropriate. Table 3 lists SP 800-53's 18 control families and the 198 recommended controls.

Table 3: NIST 800-53, Revision 3, Security Control Families and Associated Recommended Controls

Control family	Controls
Access Control	(1) Access Control Policy and Procedures, (2) Account Management, (3) Access Enforcement, (4) Information Flow Enforcement, (5) Separation of Duties, (6) Least Privilege, (7) Unsuccessful Login Attempts, (8) System Use Notification, (9) Previous Logon (Access) Notification, (10) Concurrent Session Control, (11) Session Lock, (12) Permitted Actions without Identification or Authentication, (13) Security Attributes, (14) Remote Access, (15) Wireless Access, (16) Access Control for Mobile Devices, (17) Use of External Information Systems, (18) User-Based Collaboration and Information Sharing, and (19) Publicly Accessible Content.
Awareness and Training	(1) Security Awareness and Training Policy and Procedures, (2) Security Awareness, (3) Security Training, (4) Security Training Records, and (5) Contacts with Security Groups and Associations.
Audit and Accountability	(1) Audit and Accountability Policy and Procedures, (2) Auditable Events, (3) Content of Audit Records, (4) Audit Storage Capacity, (5) Response to Audit Processing Failures, (6) Audit Review, Analysis, and Reporting, (7) Audit Reduction and Report Generation, (8) Time Stamps, (9) Protection of Audit Information, (10) Non-repudiation, (11) Audit Record Retention, (12) Audit Generation, (13) Monitoring for Information Disclosure, and (14) Session Audit.
Security Assessment and Authorization	(1) Security Assessment and Authorization Policies and Procedures, (2) Security Assessments, (3) Information System Connections, (4) Plan of Action and Milestones, (5) Security Authorization, and (6) Continuous Monitoring.

[17]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

[18]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 3 (Gaithersburg, Md.: May 2010).

Control family	Controls
Configuration Management	(1) Configuration Management Policy and Procedures, (2) Baseline Configuration, (3) Configuration Change Control, (4) Security Impact Analysis, (5) Access Restrictions for Change, (6) Configuration Settings, (7) Least Functionality, (8) Information System Component Inventory, and (9) Configuration Management Plan.
Contingency Planning	(1) Contingency Planning Policy and Procedures, (2) Contingency Plan, (3) Contingency Training, (4) Contingency Plan Testing and Exercises, (5) Alternate Storage Site, (6) Alternate Processing Site, (7) Telecommunications Services, (8) Information System Backup, and (9) Information System Recovery, and Reconstitution.
Identification and Authentication	(1) Identification and Authentication Policy and Procedures, (2) Identification and Authentication (Organizational Users), (3) Device Identification and Authentication, (4) Identifier Management, (5) Authenticator Management, (6) Authenticator Feedback, (7) Cryptographic Module Authentication, and (8) Identification and Authentication (Non-Organizational Users).
Incident Response	(1) Incident Response Policy and Procedures, (2) Incident Response Training, (3) Incident Response Testing and Exercises, (4) Incident Handling, (5) Incident Monitoring, (6) Incident Reporting, (7) Incident Response Assistance, and (8) Incident Response Plan.
Maintenance	(1) System Maintenance Policy and Procedures, (2) Controlled Maintenance, (3) Maintenance Tools, (4) Non-Local Maintenance, (5) Maintenance Personnel, and (6) Timely Maintenance.
Media Protection	(1) Media Protection Policy and Procedures, (2) Media Access, (3) Media Marking, (4) Media Storage, (5) Media Transport, and (6) Media Sanitization.
Physical and Environmental Protection	(1) Physical and Environmental Protection Policy and Procedures, (2) Physical Access Authorizations, (3) Physical Access Control, (4) Access Control for Transmission Medium, (5) Access Control for Output Devices, (6) Monitoring Physical Access, (7) Visitor Control, (8) Access Records, (9) Power Equipment and Power Cabling, (10) Emergency Shutoff, (11) Emergency Power, (12) Emergency Lighting, (13) Fire Protection, (14) Temperature and Humidity Controls, (15) Water Damage Protection, (16) Delivery and Removal, (17) Alternate Work Site, (18) Location of Information System Components, and (19) Information Leakage.
Planning	(1) Security Planning Policy and Procedures, (2) System Security Plan, (3) Rules of Behavior, (4) Privacy Impact Assessment, and (5) Security-Related Activity Planning.
Personnel Security	(1) Personnel Security Policy and Procedures, (2) Position Categorization, (3) Personnel Screening, (4) Personnel Termination, (5) Personnel Transfer, (6) Access Agreements, (7) Third-Party Personnel Security, and (8) Personnel Sanctions.
Risk Assessment	(1) Risk Assessment Policy and Procedures, (2) Security Categorization, (3) Risk Assessment, and (4) Vulnerability Scanning.
System and Services Acquisition	(1) System and Services Acquisition Policy and Procedures, (2) Allocation of Resources, (3) Life Cycle Support, (4) Acquisitions, (5) Information System Documentation, (6) Software Usage Restrictions, (7) User-Installed Software, (8) Security Engineering Principles, (9) External Information System Services, (10) Developer Configuration Management, (11) Developer Security Testing, (12) Supply Chain Protection, (13) Trustworthiness, and (14) Critical Information System Components.
System and Communications Protection	(1) System and Communications Protection Policy and Procedures, (2) Application Partitioning, (3) Security Function Isolation, (4) Information in Shared Resources, (5) Denial of Service Protection, (6) Resource Priority, (7) Boundary Protection, (8) Transmission Integrity, (9) Transmission Confidentiality, (10) Network Disconnect, (11) Trusted Path, (12) Cryptographic Key Establishment and Management, (13) Use of Cryptography, (14) Public Access Protections, (15) Collaborative Computing Devices, (16) Transmission of Security Attributes, (17) Public Key Infrastructure Certificates, (18) Mobile Code, (19) Voice Over Internet Protocol, (20) Secure Name/Address Resolution Service (Authoritative Source), (21) Secure Name/Address Resolution Service (Recursive or Caching Resolver), (22) Architecture and Provisioning for Name/Address Resolution Service, (23) Session Authenticity, (24) Fail in Known State, (25) Thin Nodes, (26) Honeypots, (27) Operating System-Independent Applications, (28) Protection of Information at Rest, (29) Heterogeneity, (30) Virtualization Techniques, (31) Covert Channel Analysis, (32) Information System Partitioning, (33) Transmission Preparation Integrity, and (34) Non-Modifiable Executable Programs.

Control family	Controls
System and Information Integrity	(1) System and Information Integrity Policy and Procedures, (2) Flaw Remediation, (3) Malicious Code Protection, (4) Information System Monitoring, (5) Security Alerts, Advisories, and Directives, (6) Security Functionality Verification, (7) Software and Information Integrity, (8) Spam Protection, (9) Information Input Restrictions, (10) Information Input Validation, (11) Error Handling, (12) Information Output Handling and Retention, and (13) Predictable Failure Prevention.
Program Management	(1) Information Security Program Plan, (2) Senior Information Security Officer, (3) Information Security Resources, (4) Plan of Action and Milestones Process, (5) Information System Inventory, (6) Information Security Measures of Performance, (7) Enterprise Architecture, (8) Critical Infrastructure Plan, (9) Risk Management Strategy, (10) Security Authorization Process, and (11) Mission/Business Process Definition.

Source: NIST SP 800-53, Revision 3.

DHS's National Cyber Security Division's Control Systems Security Program has also issued recommended practices to reduce risks to industrial control systems within and across all critical infrastructure and key resources sectors. For example, in April 2011, the program issued the *Catalog of Control Systems Security: Recommendations for Standards Developers,* which is intended to provide a detailed listing of recommended controls from several standards related to control systems.[19]

Wide Variety of Sector Cybersecurity Guidance Is Available

A wide variety of cybersecurity guidance from national and international organizations is available to critical infrastructure sector entities. Much of this guidance is tailored to the unique characteristics of each sector. Further, entities within regulated subsectors have specific cybersecurity guidance that is required or recommended to be used,[20] while entities operating outside of a regulatory environment have standards and guidance available, but not required, for their use. Furthermore, industry regulators, associations, and other groups have also developed and issued voluntary guidance available for use by entities within their respective sectors that is tailored to the business needs of entities or provides methods to address unique risks or operations.

While SCC representatives confirmed lists of cybersecurity guidance that they stated was used within their respective sectors, the representatives

[19]DHS, National Cyber Security Division, Control Systems Security Program, *Catalog of Control Systems Security: Recommendations for Standards Developers* (April 2011).

[20]Regulated subsectors include depository institutions in the banking and finance sector; bulk power system in the energy sector; and nuclear power plants in the nuclear reactors, materials, and waste sector.

emphasized that the lists were not comprehensive and that additional standards and guidance are likely used within the sectors. In addition, SCC representatives stated that they were not always aware of the extent to which the identified guidance was used by entities within their sectors.

The following discussion describes cybersecurity guidance identified for each of the sectors in our review. A list of specific guidance for each sector is provided in appendix II.

Banking and finance sector: The guidance documents for the banking and finance sector are diverse. For example, federal regulatory entities within the various sector segments issue specific risk-based cybersecurity requirements. In addition, financial institutions and the payment card industry have developed voluntary standards and practices.

FFIEC has issued handbooks that outline cybersecurity requirements for depository institutions within the sector. In addition, federal financial regulators have issued regulations that cover a comprehensive set of high-level requirements, including security programs, risk management, data security, incident response and anti-identity-theft. These regulations are in response to laws such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

The banking and finance sector-specific plan identified applicable laws, regulations, and a multitude of sector-specific guidance, especially for depository and financial institutions, that covered many cybersecurity topics such as access control authentication and phishing. Each of the FFIEC agencies often issues guidance that is similar in content but tailored to meet its legal requirements. The agencies deliver this guidance through their respective transmittal documents, such as bulletins, financial institution letters, letters to credit unions, and supervisory letters. In addition, according to an SCC representative familiar with cybersecurity guidance associated with the sector, the revision associated with the latest sector-specific plan will have more guidance on the investments and securities subsector.

Communications sector: The guidance documents for the communications sector cover a variety of topics such as telecommunication industry security standards, network engineering standards, and security configuration guides. The SCC representatives familiar with cybersecurity guidance associated with the sector stated that the identified guidance is all widely used within the sector. In addition, the representatives acknowledged that a number of the documents are

overlapping and cover similar areas, and that on the basis of its particular needs an entity may select among several. Further, decisions on whether or not to implement a specific practice within guidance depend on the role of the responsible implementer (e.g., service provider, network operator, or equipment supplier) and an understanding of the impact on factors such as the systems, networks, and organizations.

According to SCC representatives responsible for cybersecurity efforts, cybersecurity standards and practices promoted and used by SCC members include those developed by the Alliance for Telecommunications Industry Solutions, Internet Engineering Task Force, and the International Telecommunication Union. For example, the Alliance for Telecommunications Industry Solutions issued a *U.S. Standard for Signaling Security–Security Roadmap*.

In addition, the Communications Security, Reliability, and Interoperability Council[21] recently published a key guidance document to update and combine a large body of sector cybersecurity practices from a variety of sources.[22] The guidance addresses the following areas: identity management, encryption, vulnerability management, and incident response for wireless, Internet protocol services, network, people, and legacy services. The document includes 397 cybersecurity practices intended to ensure the security of networks and systems for all segments of the communications industry. According to the document, the practices are not overly prescriptive, allowing network service providers, operators, and equipment suppliers enough latitude to make deployment decisions that best suit their business practices, which revolve around technology, capability, and customer requirements.

Energy sector: The energy sector is divided between the electricity and oil and natural gas subsectors. Within the electricity subsector, the Federal Energy Regulatory Commission (FERC) certified the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization that is responsible for developing reliability

[21]The Communications Security, Reliability, and Interoperability Council is an advisory committee whose purpose is to provide recommendations to the Federal Communications Commission to ensure optimal security, reliability, and interoperability of communications systems.

[22]Communications Security, Reliability and Interoperability Council (CSRIC), *Cyber Security Best Practices* (March 2011).

standards, subject to FERC oversight, review, and approval.[23] If approved, the standards become mandatory and enforceable in the contiguous 48 states. NERC developed eight cybersecurity standards, which FERC approved in 2008,[24] that address the following topics: critical cyber asset identification, security management controls, personnel and training, electronic security perimeter(s),[25] physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets. NERC also publishes security guidelines for companies to consider for protecting electric infrastructure systems, although such guidelines are voluntary and are typically not checked for compliance. For example, NERC's June 2010 *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets* is intended to assist entities in identifying and developing a list of critical cyber assets as described in the mandatory standards.

Cybersecurity guidance for the oil and natural gas subsector has been issued by various related organizations, as has applicable guidance from closely related sectors, such as transportation and chemical. Among others, sector-specific guidance was identified from the American Petroleum Institute, American Gas Association, and the Interstate Natural Gas Association of America. For example, the American Petroleum Institute's *Security Guidelines for the Petroleum Industry* address cyber/information technology in the petroleum industry and endorse the ISO/IEC international standard 17799 for creating a cybersecurity

[23]NERC was certified in 2006 by the Federal Energy Regulatory Commission as the Electric Reliability Organization under section 215 of the Federal Power Act, as amended by the Energy Policy Act of 2005. In doing so, FERC authorized NERC to develop and enforce reliability standards for the bulk power system in the continental United States under the commission's oversight. NERC's mission is to ensure the reliability of the North American bulk power system. In addition to developing and enforcing reliability standards, NERC assesses adequacy annually via a 10-year forecast, including summer and winter forecasts; monitors the bulk power system; and educates, trains, and certifies certain industry personnel.

[24]According to FERC representatives, FERC has authority to order NERC to submit a proposed reliability standard or a modification to an existing standard to address a specific matter. Regarding the eight approved cybersecurity standards, the commission concurrently directed NERC to improve the standards through modification. The FERC representatives stated that most of the modifications have not yet been completed.

[25]An electronic security perimeter is the logical border surrounding a network to which critical cyber assets are connected and for which access is controlled.

program as voluntary guidance.[26] The other cybersecurity guidance covered various topics, including cryptography, third-party connections, and control systems.

Health care and public health sector: Cybersecurity guidance for the health care and public health sector covers a variety of topics specific to the security of health information. For example, ISO and ASTM International have issued health sector cybersecurity guidance.[27] ISO issued guidance for security management in health, and ASTM International issued guidance on user authentication and authorization. Also, according to a sector coordinating council representative, Electronic Data Interchanges are critical to data exchange within the sector and have cybersecurity implications.[28] In addition, according to the health care and public health sector annual report, the sector is engaged in an international effort to develop standardized security guidelines for health information technology that will facilitate the confidentiality, availability, and integrity of health information systems and the data residing on those systems.

The chairperson of the Healthcare and Public Health SCC stated that the sector uses Health Insurance Portability and Accountability Act of 1996 (HIPAA)-related cybersecurity guidance.[29] For example, NIST issued cybersecurity guidance to help implement the health sector's security standards included in the HIPAA security rule.[30] The NIST guidance maps the requirements in the security rule to NIST publications on information security, including typical activities an agency should consider in

[26]The reference number for ISO/IEC 17799 has changed to ISO/IEC 27002. According to ISO, the technical content is identical.

[27]ASTM International was previously known as the American Society of Testing and Materials.

[28]Electronic Data Interchanges are the computer-to-computer interchange of strictly formatted messages, also called transaction sets, that represent documents other than monetary instruments.

[29]Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 262 (Aug. 21, 1996), as amended, calls for the control of the distribution and exchange of health care data and adoption of electronic data exchange standards to uniformly and securely exchange patient information.

[30]The Department of Health and Human Services issued the Security Standards for the Protection of Electronic Protected Health Information, commonly known as the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164).

implementing an information security program. In addition, a Department of Health and Human Services (HHS) Office for Civil Rights official familiar with health information privacy issues said that the department developed guidance on how to develop a risk-based approach for protecting electronic health information and is working with NIST to develop a self-assessment tool that entities in the health sector can use to assess their security posture.

Information technology sector: Cybersecurity guidance for the information technology sector covers a number of topics, including security management system requirements, operational security, and identity management. Also, the information technology sector's 2010 sector annual report and information provided by DHS's National Protection and Programs Directorate reference the following organizations as providing cybersecurity guidance relevant to the sector:[31]

- the Internet Engineering Task Force, an international organization that develops Internet standards and protocols;[32]
- ISO/IEC, which provides standards and practices for managing information security systems;
- the Institute of Electrical and Electronics Engineers, which establishes standards and practices for managing information security systems;[33] and
- NIST, which issues special publications and interagency reports.

According to the chairperson of the IT SCC, the IT sector is very complex and there is no "short list" of cyber standards. From the industry's

[31]DHS, *2010 Sector CIKR Protection Annual Report for the Information Technology Sector* (June 2010).

[32]The Internet Engineering Task Force is a voluntary standards body that develops technical standards for the Internet including the Domain Name System protocol and its security extensions and the current and next-generation versions of the Internet Protocol.

[33]The Institute of Electrical and Electronics Engineers (IEEE) is a professional association that develops technical consensus-based electrical, engineering, and cybersecurity-related standards.

perspective, there is an "ecosystem of cybersecurity standards" that includes many different components, comprising hundreds, or even thousands, of individual standards related to technologies, practices, and products and that perform a variety of functions such as enabling interoperability and assurance of security policies and controls. Further, the standards ecosystem constantly evolves in response to new technologies, cyber threats and risks, and business models. The SCC chairperson confirmed the identified cybersecurity guidance, as shown in appendix II, as an illustrative list containing examples of cybersecurity guidance available to sector entities.

Nuclear reactors, materials, and waste sector: The cybersecurity-specific guidance for this sector includes documents issued by the Nuclear Regulatory Commission (NRC) and Nuclear Energy Institute. SCC representatives stated that the NRC and Nuclear Energy Institute guidance documents were widely used for nuclear power plants within the sector. NRC, under its regulatory authority, requires, among other things, that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Both NRC and the institute have issued guidance containing methods that entities may use to meet the regulatory requirements. This guidance includes NRC's Regulatory Guide 5.71 for cybersecurity programs at nuclear facilities,[34] the most recent version of which was issued in January 2010, and the institute's cybersecurity plan for nuclear power reactors,[35] the most recent version of which was issued in April 2010. NRC officials and institute representatives familiar with both guides stated that they contain similar cybersecurity controls. However, these guides are not substitutes for compliance with regulations, and compliance with the guides is not mandatory. According to NRC representatives responsible for NRC's cybersecurity-related efforts, the guides provide an approach that the NRC staff deems acceptable for complying with the commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack. Although licensees may use methods other than those described within this guidance to meet the commission's regulations, the NRC representatives said that all licensees have used one of these two

[34]NRC Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities* (January 2010).

[35]NEI 08-09, Revision 6, *Cyber Security Plan for Nuclear Power Reactors* (April 2010).

methods. In addition, the NRC representatives said that they are developing a new guide to facilitate inspections of cybersecurity programs.

NRC's cybersecurity regulations are currently only applicable to power-generating facilities. The NRC representative familiar with cybersecurity guidance said that, in general, NRC's rule-making process is based on the risk to the public and has included the issuance of regulations for the power generation facilities first, which are then typically promulgated to fuel cycle facilities,[36] and then to other nuclear facilities (such as research reactors), as needed. Also, NRC issued a series of orders recommending greater cybersecurity after September 11, 2001.

According to the 2010 sector annual report, the Nuclear Sector Cyber Subcouncil is working on a road map to secure control systems in the nuclear sector. The annual report states that the road map will build on existing government and industry efforts to enhance the security of control systems in the power and nonpower reactor segments of the sector, taking into account NRC's cybersecurity requirements. According to a DHS official, the scope of the road map was limited to commercial nuclear power plants.[37]

Water sector: Cybersecurity guidance for the water sector covers a number of topics, including risk analysis and management and industrial control systems. However, information compiled from the SCC membership and provided by the Secretariat of the Water SCC showed that several documents cited as relevant to cybersecurity were not widely used by entities within the sector for various reasons, including the lack of resources and funding to implement a cybersecurity program. The representatives further stated that while the larger utilities have the staffing levels and budgets that enable them to more fully implement cybersecurity for their control systems, many medium-size or small utilities struggle to maintain the staff needed just to keep their systems properly running.

[36]Fuel cycle facilities manufacture fuel such as uranium for nuclear reactors.

[37]According to a DHS official, the *Roadmap to Enhance Cyber Systems Security in the Nuclear Sector* was approved in October 2011.

Furthermore, Water SCC representatives familiar with cybersecurity guidance associated with the sector said that while they have not specified any specific cybersecurity guidance that water utilities are to use, some utilities are using and implementing cybersecurity guidance that has been used in other sectors. Also, the Cybersecurity Working Group of the Water SCC prepared with DHS a road map to define gaps and a strategy for addressing outstanding needs in securing process control systems. It states that planned cybersecurity activities include (1) isolating control systems from public switched networks and (2) adopting recommended practices for control systems in the water sector.

Cross-sector guidance: In addition to sector-specific guidance, cybersecurity guidance from national and international organizations can be and is utilized by sector entities and was frequently mentioned as important in developing sector-specific guidance. These include NIST's risk management framework and security controls for information systems and industrial control systems; DHS's recommended security controls for control systems; ISO guidance on establishing an information system security control program, including security control guidance; and the International Society of Automation's security guidance for industrial control systems.

Implementation of Cybersecurity Can Be Enforced through a Variety of Mechanisms, but More Could Be Done to Disseminate and Promote Guidance

Implementation of cybersecurity guidance can occur through a variety of mechanisms, including enforcement of regulations and voluntarily in response to business incentives; however, responsible federal entities could take additional steps to promote the most applicable and effective guidance throughout the sectors. Entities operating under a federal regulatory environment are required to adhere to cybersecurity standards to meet their regulatory requirements or face enforcement mechanisms. Entities not subject to regulation do not face such enforcement mechanisms, but may voluntarily implement cybersecurity guidance in response to business incentives, such as mitigating risk, ensuring interoperability among systems, or protecting intellectual property. With respect to promoting cybersecurity guidance, sector-specific agencies, and, in particular, DHS, have specific roles to play in coordinating cybersecurity efforts, which include the promotion and dissemination of guidance and practices. While DHS and other agencies have taken a number of steps in this area, more could be done to identify guidance and standards applicable to entities within the sectors and to promote their implementation.

Regulated Entities Are Required to Comply with Federal Cybersecurity Regulations or Face Enforcement Actions

Critical infrastructure entities covered under regulation, such as depository institutions in the banking and finance sector; the bulk power system in the electricity subsector of the energy sector; health care and public health sector; and the nuclear reactors, materials, and waste sector, are regulated by the federal government and thus are required to meet mandatory cybersecurity standards established by regulation under federal law.[38] When an entity is determined to be not compliant with these requirements, various types of enforcement mechanisms can be employed. These mechanisms include administrative actions such as a supervisory directive or memorandum of understanding. More severe enforcement actions include cease and desist orders, remedial directives, revocations of license or certification, and civil monetary penalties.

Depository Institutions (Banking and Finance Sector)

Cybersecurity oversight functions are conducted by FFIEC member agencies through examinations.[39] According to the FFIEC IT Subcommittee Chairperson, for most larger financial institutions, examiners have a continuous, on-site presence and are constantly evaluating their assigned financial institutions' programs, in particular in regard to cybersecurity, which is considered high risk, to ensure that the institutions operate safely and soundly. For smaller financial institutions, examinations for cybersecurity risks occur every 12 to 18 months or after the issuance of significant regulatory guidance.

Each regulatory agency has its own enforcement policies. In general, enforcement mechanisms include both informal and formal enforcement actions. Informal enforcement actions are used when a financial institution's overall condition is sound, but written commitments from the board of directors are needed to ensure that it will correct problems and

[38]In September 2008, we reported that there are at least 34 federal laws, regulations, and mandatory standards that pertain to securing privately owned IT systems and data in our nation's critical infrastructure sectors and each of the 34 federal legal requirements has at least one enforcement mechanism. See GAO-08-1075R.

[39]For example, the Federal Deposit Insurance Corporation can initiate enforcement actions and orders against state nonmember banks, and insured foreign banks. The National Credit Union Administration can initiate enforcement actions and orders against federally insured credit unions and credit union–affiliated parties. The Office of the Comptroller of the Currency can initiate enforcement actions and orders against national banks and federal savings associations, federally chartered branches, and agencies of foreign banks. The Federal Reserve System can initiate enforcement actions and orders against state member banks; financial, bank, and thrift holding companies; and U.S. operations of foreign banking organizations.

weaknesses identified by the examiners. Informal enforcement actions can consist of the following:

- a memorandum of understanding or document of resolution,
- board resolution,
- a supervisory directive,
- a notice of deficiency and request for a safety and soundness compliance plan, or
- individual minimum capital requirement directives.

Formal actions are authorized by statute and mandated in some cases, are generally more severe, and are disclosed to the public. Depending on whether the institution is a credit union or a bank, formal enforcement actions for any violations of laws and regulations, including various cybersecurity provisions, can take the following forms:

- cease and desist orders,
- conservatorships and receiverships,[40]
- civil money penalties,
- termination of insurance, and
- liquidation.

For example, an agency can assess civil monetary penalties of $7,500 per day for any violation of law or regulation, or assess a fine up to $37,000 per day for a violation that is, for instance, likely to cause more than a minimal loss to the financial institution, or assess a penalty of up to $1,375,000 million per day for knowingly engaging, for instance, in any unsafe or unsound practice when the offender knowingly or recklessly

[40]Conservatorship preserves the value of the failed institution as an operating financial institution until it can be returned to normal operations or final resolution can be accomplished through a merger, purchase and assumption, or liquidation. Receivership is the orderly administration of the failed bank's assets and liabilities.

caused a substantial loss to the financial institution or received a substantial pecuniary gain or other benefit. However, according to the FFIEC IT Subcommittee Chairperson, while depository institutions have been cited for operating in an unsafe and unsound manner as it relates to cybersecurity, none of these cases have reached the level of formal actions with civil monetary penalties.

Bulk Power System (Electricity Subsector of the Energy Sector)

NERC, as the Electric Reliability Organization, has the authority to enforce compliance with mandatory cybersecurity standards through its Compliance Monitoring and Enforcement Program, subject to FERC review.[41] While FERC has authorized NERC to enforce mandatory reliability standards in the United States, the commission retains its own authority to enforce the same standards and assess penalties for violations. The commission also has the ability to review each penalty NERC proposes for noncompliance with a reliability standard in the United States, either by its own action or upon an appeal by a penalized entity.

Monitoring functions are carried out by NERC inspectors through a number of actions:

- Performing compliance audits for bulk power system owners, operators, and users on a schedule established by NERC.
- Periodically conducting a self-certification to attest to compliance or noncompliance with reliability standards.
- Initiating spot checks or performing compliance violation investigations in response to an event or complaint.
- Encouraging self-reporting versus formal NERC reporting when a user, owner, or operator of the bulk power system becomes aware of a violation of a reliability standard or of a change in the violation severity level of a previously reported violation.

[41]According to NERC's Rules of Procedures, NERC shall develop and implement a Compliance Monitoring and Enforcement Program to promote the reliability of the bulk power system by enforcing compliance with approved reliability standards in those regions of North America in which NERC has been given enforcement authority.

- Requiring periodic data submissions. Under this circumstance, a team of industry experts is established to review the data and provide a report to NERC.

- Requiring technical feasibility exception reporting for the reliability standards that allow such exceptions. Those reliability standards require reporting of exceptions to compliance with the reliability standard and approval by NERC of the exceptions as a form of compliance monitoring.

- Reviewing complaints received alleging violations of a reliability standard to determine if a compliance violation investigation is required.

Enforcement mechanisms include monetary penalties, nonmonetary sanctions, and remedial actions, according to NERC sanction guidelines. NERC can levy monetary penalties for the violation of requirements of the reliability standards. For example, NERC or regional entities,[42] upon delegation of NERC's authority, can impose a monetary penalty or fine of up to $1 million per day per violation, depending on the risk factors and level of violation severity involved.[43] NERC must file all penalties it or a regional entity proposes to impose with FERC. If FERC takes no action after 31 days, the penalties go into effect, or FERC can either reject or take up the proposed penalty for further action. Entities can appeal the penalties with FERC.

For the month of July 2011, a Notice of Penalty was issued for violations of NERC Cyber Security Standards, one of which included a high violation risk factor that had a monetary penalty of $75,000 imposed, according to NERC's publicly available enforcement information on penalties.[44] In addition, there were 65 cybersecurity violations with a medium violation risk factor reported that had total monetary penalties of

[42]NERC works with eight regional entities to improve the reliability of the bulk power system. The members of the regional entities come from all segments of the electric industry. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Mexico.

[43]FERC also has authority to impose penalties for violations of the reliability standards it has approved, including violations of the eight Cyber Security Standards.

[44]Enforcement information is publicly available on NERC's website and has been filed as part of a Notice of Penalty with the Federal Energy Regulatory Commission.

approximately $496,000 imposed and 24 cybersecurity violations with a low violation risk factor that had total monetary penalties of approximately $375,000 imposed.

NERC, the regional entities, and FERC can also levy nonmonetary sanctions against a violator that include limitations or restrictions that may result in economic or other impacts. In addition to monetary and nonmonetary sanctions, NERC, the regional entities, and FERC can direct bulk power system entities to take remedial action to correct conditions, practices, or any other relevant action or activity underlying the noncompliance involved, including cybersecurity-related issues. For example, remedial actions may include the following:

- specifying operating or planning criteria, limits, or limitations;
- requiring specific system studies;
- defining operating practices or guidelines;
- requiring confirmation of data, practices, or procedures through inspection testing or other methods;
- requiring specific training for personnel; and
- requiring development of specific operating plans.

Health Care and Public Health Sector

HHS's Office for Civil Rights (OCR) is responsible under HIPAA for oversight and enforcement of the protection of electronic protected health information held by covered entities within the health care and public health sector. Cybersecurity requirements are also applicable to this sector's reimbursement and supply chain functions.

Oversight of HIPAA's Security Rule is carried out through compliance reviews and complaints that can be received through one of HHS's 10 regional offices.[45] According to an OCR official familiar with health information privacy issues, HHS has undertaken oversight of Security Rule compliance. For example, during calendar year 2010, HHS reported opening 243 complaints and compliance reviews involving Security Rule

[45]The Security Rule establishes national standards to protect electronic protected health information created, transmitted, or maintained by a covered entity.

issues, which represents a 95 percent increase in the number of Security Rule cases opened over the average caseload of the previous 4 years. In addition, OCR reported resolving a total of 128 complaints, which is an increase of 16 percent over the average number of resolved complaints in the previous 4 years. More importantly, 55 percent of the resolved complaints required the regulated entity to take corrective action to achieve compliance with the Security Rule, whereas on average only 18 percent of the resolved complaints in prior years required such action.[46]

Additionally, HIPAA-covered entities and their business associates are to provide notification following a breach of unsecured protected health information.[47] Under the Health Information Technology for Economic and Clinical Health Act's Breach Notification Interim Final Rule, OCR processes and initiates investigations of reports involving 500 or more individuals. According to the OCR health information privacy official, since the inception of the breach notification requirement, over 70 percent of the 280 major breaches reported (as of May 30, 2011) involved electronic protected health information, and thus required investigation for Security Rule compliance. Of these cases, the official stated that 6 percent of breach reports involving more than 500 individuals have been due to hacking or cybersecurity incidents, compared with 67 percent of these breaches being due to the physical loss or theft of protected health information.

Enforcement mechanisms include the imposition of civil money penalties for violations. HHS can levy fines or penalties for failure to comply with the cybersecurity standards or specifications of the Security Rule, Privacy Rule,[48] and Breach Notification Interim Final Rule.

[46]Department of Health and Human Services, Office for Civil Rights, "Health Information Security Rule Trends in Enforcement" (briefing presented at the NIST/OCR HIPAA Security Assurance Conference, Washington, D.C.: May 11, 2011).

[47]Breach notification was implemented under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

[48]The HIPAA Privacy Rule establishes national standards to protect an individual's medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

When considering civil monetary penalties, there are four categories of violations that reflect increasing levels of culpability. The categories and minimum penalties are as follows:

- Did not know $100
- Reasonable cause $1,000
- Willful neglect—corrected $10,000
- Willful neglect—not corrected $50,000

For each violation, the maximum penalty amount in every category is $50,000. For multiple violations in a calendar year, the maximum penalty amount in each category is $1.5 million. HHS determines the penalty amounts based on the nature and extent of the violation, resulting harm, and other factors.

The OCR health information privacy official also indicated that the office has executed resolution agreements and corrective action plans in several cases where investigation has found systemic failures to comply with the Security Rule for protecting electronic health information. For example, the official stated that OCR executed a resolution agreement with a major university in the amount of $865,000, which also included a 3-year corrective action plan to implement stronger safeguards for electronic protected health information as well as comprehensive employee training on the appropriate use of patient information. In another case, OCR executed a resolution agreement with a major hospital in the amount of $1 million that included a 3-year corrective action plan to address stronger safeguards for the removal of protected health information from the hospital by employees for work-related purposes, including the removal of electronic protected health information.

Nuclear Reactors (Nuclear Reactors, Materials, and Waste Sector)

NRC is responsible for both physical security and cybersecurity oversight. To enhance its current cybersecurity program, NRC has issued a cybersecurity-focused regulation[49] and a cybersecurity regulatory guide.[50]

Current cybersecurity oversight functions are carried out through inspections of licensed facilities to ensure that they are in compliance with NRC regulations and the terms of their licenses. Although NRC has not imposed a civil penalty for cybersecurity violations at its facilities under its current enforcement policy, failure to comply with NRC's regulations may result in the imposition of enforcement sanctions such as notices of violation, civil penalties, and the issuance of orders.

Prior to implementing its new cybersecurity program, NRC must review and approve the cybersecurity plans for all operational nuclear power plants. Once a cybersecurity plan is approved for a particular nuclear power plant, implementing the program defined within that plan becomes both a condition of that plant's operating license and an inspection requirement.

In addition to approving cybersecurity plans, NRC is also developing a cybersecurity inspection program that is scheduled for implementation during 2012 and is in the early stages of revising its cybersecurity enforcement policy to account for the new cybersecurity inspection program. The cybersecurity inspection program will be implemented in three stages. In the first stage, NRC intends to develop its initial inspection guidance. In the second stage, NRC intends to commence specialized inspector cybersecurity training and education in preparation for on-site cybersecurity inspections at licensed facilities. In the final stage, NRC will leverage the results of and the insights gained from its initial inspections to develop program guidance and procedures for future periodic inspections.

Finally, NRC is in the early stages of revising its cybersecurity enforcement policy to account for the new cybersecurity inspection program.

[49]10 CFR §73.54, Protection of Digital Computer and Communication Systems and Networks, March 2009.

[50]NRC Regulatory Guide 5.71, *Cyber Security Program for Nuclear Facilities* (January 2010).

Although No Enforcement Mechanisms Exist, Nonregulated Entities Have Business Reasons to Implement Cybersecurity Based on Available Guidance

According to officials familiar with cybersecurity issues in their respective SCCs, the information technology, communications, and water critical infrastructure sectors and oil and natural gas subsector of the energy sector are not subject to direct federal cybersecurity-related regulation.[51]

Although the use of cybersecurity guidance is not mandatory, entities may voluntarily implement such guidance in response to business incentives, including to mitigate risks, protect intellectual property, ensure interoperability among systems, and encourage the use of leading practices. For example, officials familiar with cybersecurity issues from both the communications sector and information technology sector stated that the competitive market place, desire to maintain profits, and customer expectation of information security—rather than federal regulation—drive the adoption of best practices. Oil and gas SCC officials said that their member companies are not required to follow industry guidelines, but legal repercussions regarding standard of care may motivate the incorporation of such cybersecurity standards into their operations.

DHS and Sector-Specific Agencies Have Taken Steps to Disseminate and Promote Guidance, but More Could Be Done

As recognized in federal policy, the dissemination and promotion of cybersecurity standards and guidance is a goal in enhancing the security of our nation's cyber-reliant critical infrastructure. The NIPP states that, in accordance with HSPD-7, DHS is a principal focal point for the security of cyberspace and is responsible for coordinating efforts to protect the cyber infrastructure to ensure its confidentiality, integrity, and availability. These responsibilities, among other things, include providing guidance on effective cyber-protective measures, assisting the sector-specific agencies in understanding and mitigating cyber risk, and assisting in developing effective and appropriate protective measures. To accomplish these responsibilities, DHS is to help in the development of comprehensive cybersecurity guidance that homeland security partners may adopt to meet accepted industry-based standards that measurably reduce the risk of cyber disruption or exploitation.

[51]In commenting on the draft report, an Oil and Natural Gas Subsector Coordinating Council representative familiar with cybersecurity-related regulation stated that entities in the oil and natural gas subsector that have high-risk chemical facilities are subject to Chemical Facility Anti-Terrorism Standards. Facilities covered by this standard are required to implement measures to deter cyber sabotage, and prevent unauthorized onsite or remote access to critical process controls systems, critical business systems, and sensitive computerized systems.

In this regard, DHS and the other sector-specific agencies for the sectors selected for review have disseminated and promoted cybersecurity guidance among and within sectors. For example, officials from DHS's National Cybersecurity Division (NCSD) stated that they work within the public-private partnership model to identify and prioritize cybersecurity risks within sectors, then coordinate with the sectors to encourage entities to adopt cybersecurity guidance to mitigate identified vulnerabilities. NCSD also engages with standards-developing organizations to provide input, resources, and support. For example, NCSD has provided resources, including time and expertise, supporting the development of security standards with NIST, ANSI, ISO, and the International Telecommunication Union. In addition, NCSD leverages a variety of resources to promote specific cybersecurity standards and practices. For example, through its Control Systems Security Program, NCSD has taken several actions, such as developing a catalog of recommended security practices for control systems, developing a cybersecurity evaluation tool that allows asset owners to assess their control systems and overall security posture, and collaborating with the Industrial Control Systems Joint Working Group to promote control standards and system security.

In addition, officials from the Department of Energy's Office of Electricity Delivery and Energy Reliability stated that the department, as the energy-sector-specific agency, is involved in many ongoing efforts to assist the sector in the development, assessment, and sharing of cybersecurity standards. For example, the department is working with NIST to enable state power producers to use current cybersecurity guidance. The department is also the Vice Chair of the Cyber Security Working Group and provides funds that will enable private sector power producers to share practices. In addition, according to Department of Energy officials, the department is currently leading an initiative to develop a risk management guideline for the electric grid to ensure that cybersecurity risks are addressed at the organization, mission or business process, and information system levels. This is modeled after NIST Special Publication 800-39 and tailored to the needs of the energy sector. Further, Department of Health and Human Services officials responsible for the agency's sector-specific efforts also stated that they encourage the sharing of existing standards. For example, a public-private cybersecurity

workgroup was formed that developed a cybersecurity primer to educate members of the sector.[52]

While these are significant steps, DHS and the other sector-specific agencies have not identified the key cybersecurity guidance applicable to or widely used in each of their respective critical infrastructure sectors. In addition, DHS guidance for preparing the sector-specific critical infrastructure protection plans calls for, among other things, outlining the sector's cyber protection and resilience strategies; however, these plans largely do not identify key guidance and standards for cybersecurity. Specifically, only one of the seven sectors reviewed (banking and finance) listed cybersecurity guidance in its current sector-specific plan. The other six sectors mentioned certain guidance in these plans, but did not list applicable guidance.

Sectors reported that they did not identify this guidance in their plans in part because DHS did not specifically address listing cybersecurity guidance in its guidance for the revision of the sector-specific plans. In addition, officials from DHS's NCSD noted that their engagement in the area of standards focuses on promoting standards and practices from a cross-sector perspective, rather than focusing on individual sectors. However, given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.

[52]Healthcare and Public Health Sector Cybersecurity Working Group, *Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101*.

Cybersecurity Guidance For Three Subsectors Is Substantially Similar to Federal Guidance

Sector cybersecurity guidance related to three subsectors (electricity, depository institutions, and nuclear reactors) is substantially similar[53] to guidance applicable to federal agencies.[54] Specifically, sector cybersecurity guidance and supplementary documents that we analyzed addressed most of NIST's risk management framework steps and most of the 198 recommended security controls in NIST SP 800-53 (listed in table 3) that are specified for federal information systems. In cases where differences existed in terms of security controls, sector representatives provided supplementary documents with controls that resolved the difference, or explained that some federally recommended security controls were not applicable for sector-specific reasons.

Bulk Power System (Electricity Subsector of the Energy Sector)

NERC Cyber Security Standards 002 through 009, Version 3,[55] and supplementary documents[56] are substantially similar to guidance applicable to federal agencies. As discussed previously, the NIST risk management framework describes the activities important to an effective information security program (e.g., categorize information systems, select security controls). Similarly, the NERC Cyber Security Standards provide a cybersecurity framework for the identification and protection of entity-identified critical cyber assets to support reliable operation of the bulk

[53]A similarity or commonality was determined when sector cybersecurity guidance or supplementary documents addressed a security topic with similar functionality as in federal guidance.

[54]Guidance applicable to federal agencies includes, among others, Special Publications (SP) that are developed by NIST. For purpose of comparison, we used NIST SP 800-37 Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* (February 2010) and NIST SP 800-53 Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations* (May 2010).

[55]The Chief Security Officer of NERC, who was also the Secretary of the Electricity Sub-Sector Coordinating Council, identified the NERC Cyber Security Standards as commonly used in the electricity subsector. In addition, the NERC Cyber Security Standards 002 through 009, Version 3, were approved by NERC's Board of Trustees on December 16, 2009, and by the Federal Energy Regulatory Commission on March 31, 2010, with an effective date of October 1, 2010.

[56]For example, NERC issues Security Guidelines that describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems.

power system.[57] The standards also cover eight cybersecurity areas (e.g., Security Management Controls and Systems Security Management), which contain mandatory and enforceable minimum security requirements (e.g., critical cyber asset identification and cyber vulnerability assessment).

As discussed previously, NIST SP 800-53, Revision 3, addresses one of the steps in the NIST risk management framework, which is to select a baseline of security controls and tailor and supplement the baseline based on an organizational risk assessment. SP 800-53 contains 18 control families (e.g., Access Control and Risk Assessment), which in total, contain 198 recommended security controls (e.g., Account Management and Malicious Code Protection) for federal information systems and organizations.

We determined that the eight NERC Cyber Security Standards and supplementary documents addressed 151 of the 198 SP 800-53 controls, and NERC officials responsible for the Cyber Security Standards deemed 46 of the remaining controls to be not applicable, and stated that 1 control—transmission integrity—was not considered when revising the latest NERC Cyber Security Standards. The NERC officials provided specific reasons as to why the 46 controls were not applicable to the bulk power system, as illustrated by the following examples:

- A control had the potential to increase risk to operations of bulk power system entities.
- A control was inappropriate and not feasible in a real-time control system environment.
- A control did not have universal applicability.

[57]According to a FERC representative from the Office of the Executive Director, the NERC Version 3 Cyber Security Standards provide a cybersecurity framework only for the protection of entities' self-identified "critical cyber assets." The representative added that currently, as applied by industry, most applicable entities' cyber assets are not identified for CIP protective measures. According to a NERC representative, CIP-002 Version 4, "Critical Cyber Asset Identification," which proposes to include "bright line" criteria for the identification of critical assets, was filed with FERC in February of 2011 and is pending FERC approval.

- A control based on FISMA compliance did not apply to the bulk power system environment.

Additionally, the NERC officials expressed their concerns about comparing NERC Cyber Security Standards with those of SP 800-53. They said that the authority and scope of their standards derived from Section 215 of the Federal Power Act, as amended, while SP 800-53 derived from FISMA; therefore, the intended purpose of their standards is different from that of the guidance for federal agencies. The officials also said that the NERC Cyber Security Standards are mandatory and enforceable, whereas SP 800-53 provides a menu of possibilities to choose from depending on the specific situation and relies on the concepts of compensating controls and risk management to make trade-offs.

Table 4 provides a summary of the comparison between the electricity subsector guidance and federal guidance, including the controls deemed not applicable by sector officials.

Table 4: Electricity Subsector Cybersecurity Standards and Guidance Compared with Federal Guidance

NIST control family name and number of controls	Comparison with NERC Cyber Security Standards and supplementary documents
Access Control (19)	Addresses 13 of the 19 controls, and NERC officials deemed 6 controls—Separation of Duties, Session Lock, Permitted Actions Without Identification or Authentication, Security Attributes, Access Control for Mobile Devices, Use of External Information Systems, and User-Based Collaboration and Information Sharing—to be not applicable.
Awareness and Training (5)	Addresses all 5 controls.
Audit and Accountability (14)	Addresses all 14 controls.
Security Assessment and Authorization (6)	Addresses all 6 controls.
Configuration Management (9)	Addresses all 9 controls.
Contingency Planning (9)	Addresses all 9 controls.
Identification and Authentication (8)	Addresses all 8 controls.
Incident Response (8)	Addresses all 8 controls.
Maintenance (6)	Addresses all 6 controls.
Media Protection (6)	Addresses all 6 controls.
Physical and Environmental Protection (19)	Addresses 18 of the 19 controls, and NERC officials deemed 1 control—Information Leakage—to be not applicable.
Planning (5)	Addresses 4 of the 5 controls, and NERC officials deemed 1 control—Privacy Impact Assessment—to be not applicable.
Personnel Security (8)	Addresses all 8 controls.

NIST control family name and number of controls	Comparison with NERC Cyber Security Standards and supplementary documents
Risk Assessment (4)	Addresses all 4 controls.
System and Services Acquisition (14)	Addresses 7 of the 14 controls, and NERC officials deemed 7 controls—Allocation of Resources, Life Cycle Support, Acquisitions, Software Usage Restrictions, Security Engineering Principles, Supply Chain Protection, and Trustworthiness—to be not applicable.
System and Communications Protection (34)	Addresses 9 of the 34 controls, and NERC officials deemed 24 controls—Application Partitioning, Security Function Isolation, Resource Priority, Network Disconnect, Trusted Path, Cryptographic Key Establishment and Management, Use of Cryptography, Public Access Protections, Transmission of Security Attributes, Public Key Infrastructure Certificates, Secure Name/Address Resolution Service (Authoritative Source), Secure Name/Address Resolution Service (Recursive or Caching Resolver), Architecture and Provisioning for Name/Address Resolution Service, Session Authenticity, Fail In Known State, Thin Nodes, Honeypots, Operating System-Independent Applications, Heterogeneity, Virtualization Techniques, Covert Channel Analysis, Information System Partitioning, Transmission Preparation Integrity, and Non-Modifiable Executable Programs—to be not applicable. In addition, NERC officials stated that 1 control—Transmission Integrity—was not considered when revising the latest NERC Cyber Security Standards.
System and Information Integrity (13)	Addresses 11 of the 13 controls, and NERC officials deemed 2 controls—Information Input Validation and Error Handling—to be not applicable.
Program Management (11)	Addresses 6 of the 11 controls, and NERC officials deemed 5 controls—Information Security Resources, Information Security Measures of Performance, Enterprise Architecture, Critical Infrastructure Plan, and Mission/Business Process Definition—to be not applicable.

Source: GAO analysis of electricity sector documents and interviews.

Examples of commonalities between the electricity subsector cybersecurity guidance and federal guidance, as well as the controls deemed not applicable, are described below.

Commonality: SP 800-53 recommends that personnel report suspected security incidents to the organizational incident response capability and report security incident information to designated authorities. The NERC Cyber Security Standard on Incident Reporting and Response Planning contains a similar control by requiring that the responsible entity report cybersecurity incidents to the Electricity Sector Information Sharing and Analysis Center.

Commonality: SP 800-53 recommends protecting the confidentiality of transmitted information. NERC Security Guidelines for the Electricity Sector, Protecting Potentially Sensitive Information, Version 1.0, contain a similar control by specifying that, among other things, critical infrastructure owners and operators should have an information security or confidentiality policy in place as an integral part of their business-level

policies and that the policy should address the production, storage, transmission, and disposal of both physical and electronic information.

Commonality: SP 800-53 recommends maintaining and monitoring temperature and humidity levels within the facility where the information system resides to prevent fluctuations potentially harmful to the information system. The NERC officials stated that the physical infrastructure requirements in the Emergency Preparedness and Operations Reliability Standards require backup control center functionality in the event of any kind of failure of the primary control center.

Not applicable: SP 800-53 recommends implementing a session lock control after a period of inactivity or upon receiving a request from a user. According to the NERC officials, this control is not applicable and not feasible in a real-time control system environment because session lock on an operational console could result in a loss of system operations and system monitoring, leading to a loss of present situational awareness. The NERC officials also stated that a lack of situational awareness was a key factor leading to the August 14, 2003, blackout.[58]

Not applicable: SP 800-53 recommends employing virtualization techniques to present information system components as other types of components, or components with differing configurations. According to the NERC officials, given the variety of technology and scale implemented by their members, this control would not have universal applicability.

Not applicable: SP 800-53 recommends separating duties of individuals as necessary to prevent malevolent activity without collusion. According to the NERC officials, the control is not applicable because it would have the potential to increase risk to operations of bulk power system entities. The NERC officials also stated that the electricity industry typically maintains a practice of separation of duties between IT system developers and support, but placing further separation of duties requirements on operations personnel would result in decreased operational responsiveness and reliability.

[58]The August 14, 2003, blackout was a major disturbance of portions of the power grid of the United States and Canada that affected an estimated 50 million people and resulted in the loss of more than 61,800 megawatts of electrical load.

Depository Institutions (Banking and Finance Sector)

The *FFIEC IT Examination Handbook* (IT Handbook), which is composed of 11 booklets, is substantially similar to guidance applicable to federal agencies.[59] Similar to the NIST risk management framework, the IT Handbook addresses various information technology topics (e.g., information security, operations, and management). Specifically, the Information Security Booklet is intended to provide guidance to examiners and organizations for assessing the level of security risks to the organization and evaluating the adequacy of the organization's risk management. In addition, this booklet states that financial institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks.

We determined that the IT Handbook addressed 196 of 198 SP 800-53 controls; the FFIEC officials deemed the remaining 2 controls to be not applicable. Additionally, FFIEC officials responsible for cybersecurity-related issues and guidance expressed concerns about comparing NIST guidelines with those of the IT Handbook. According to the FFIEC officials, although the general purpose for both information resources is to protect information security assets, the process by which they communicate their intended purpose is different. Specifically, according to these officials, while many NIST controls directly compare with those of the IT Handbook, the target audiences are vastly different. The IT Handbook provides a higher-level overview (i.e., risk-based principles) detailing the controls and standards, while NIST describes specific controls for a standard. Therefore, comparisons between the two sets of guidance can best be accomplished by comparing information security concepts and principles.

Table 5 provides a summary of the comparison between the banking and finance sector cybersecurity guidance and federal guidance, including the controls deemed not applicable by sector officials.

[59]The Financial Services Sector Coordinating Council identified the *FFIEC IT Examination Handbook* as cybersecurity guidance that is commonly used in the banking and finance sector. The IT Handbook addresses various topics, including (1) audit, (2) business continuity planning, (3) development and acquisition, (4) electronic banking, (5) information security, (6) management, (7) operations, (8) outsourcing technology services, (9) retail payment systems, (10) supervision of technology service providers, and (11) wholesale payment systems.

Table 5: Banking and Finance Sector Cybersecurity Guidance Compared with Federal Guidance

NIST control family name and number of controls	Comparison with the FFIEC IT handbook
Access Control (19)	Addresses 18 of the 19 controls, and FFIEC officials deemed 1 control—Permitted Actions without Identification or Authentication—to be not applicable.
Awareness and Training (5)	Addresses all 5 controls.
Audit and Accountability (14)	Addresses all 14 controls.
Security Assessment and Authorization (6)	Addresses all 6 controls.
Configuration Management (9)	Addresses all 9 controls.
Contingency Planning (9)	Addresses all 9 controls.
Identification and Authentication (8)	Addresses all 8 controls.
Incident Response (8)	Addresses all 8 controls.
Maintenance (6)	Addresses all 6 controls.
Media Protection (6)	Addresses all 6 controls.
Physical and Environmental Protection (19)	Addresses all 19 controls.
Planning (5)	Addresses all 5 controls.
Personnel Security (8)	Addresses all 8 controls.
Risk Assessment (4)	Addresses all 4 controls.
System and Services Acquisition (14)	Addresses all 14 controls.
System and Communications Protection (34)	Addresses 33 of the 34 controls, and FFIEC officials deemed 1 control—Heterogeneity—to be not applicable.
System and Information Integrity (13)	Addresses all 13 controls.
Program Management (11)	Addresses all 11 controls.

Source: GAO analysis of banking and finance sector documents and interviews.

Examples of commonalities between the banking and finance sector cybersecurity guidance and federal guidance, as well as the controls deemed not applicable, are described below.

Commonality: SP 800-53 recommends implementing a session lock control after a period of inactivity or upon receiving a request from a user. The IT Handbook contains a similar control by specifying that controls include automatically logging the workstation out after a period of inactivity and heuristic intrusion detection.

Commonality: SP 800-53 recommends usage restrictions and implementation guidance for wireless access. The IT Handbook contains a similar control by specifying that financial institutions determine whether appropriate device and session authentication takes place, particularly for remote and wireless machines.

Not applicable: SP 800-53 recommends identifying specific user actions that can be performed on the information system without identification or authentication. According to the FFIEC officials, this control is not applicable because it would be excessive and burdensome to identify user actions within systems that do not require controls to protect sensitive, classified, or nonpublic information. In addition, the Information Security Booklet provides guidance as to how access should be given (i.e., sufficient access required to perform the work to be done).

Not applicable: SP 800-53 recommends employing diverse information technologies in the implementation of the information system to reduce the impact of the exploitation of a specific technology. According to the FFIEC officials, this control is not applicable because it could add complexity and management overhead that could lead to mistakes and misconfigurations that could increase overall risk.

Nuclear Reactors (Nuclear Reactors, Materials, and Waste Sector)

NRC Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities* (RG 5.71)[60] and supplementary documents[61] are substantially similar to guidance applicable to federal agencies. According to NRC representatives responsible for NRC's cybersecurity-related efforts, RG 5.71 sets forth methods that NRC has found acceptable for licensees to use in complying with the requirements of 10 CFR §73.54. Similar to the NIST risk management framework, these methods describe the activities

[60]The Co-chair to the Nuclear Sector Cyber Security Subcouncil identified RG 5.71 as cybersecurity guidance that is commonly used in the nuclear reactors, materials, and waste sector. In addition, the Nuclear Energy Institute has developed NEI 08-09 to assist licensees in complying with the requirements of 10 CFR §73.54, and according to NEI and NRC officials, the security controls are essentially equal to those in RG 5.71.

[61]NRC promulgates regulations that are then codified in the Code of Federal Regulations (CFR) as requirements binding on all persons and organizations who receive a license from NRC to use nuclear materials or operate nuclear facilities. For example, NRC promulgates 10 CFR §73.54, *Protection of Digital Computer and Communication Systems and Networks,* which requires, in part, that U.S. Nuclear Regulatory Commission licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat. In addition, NRC issues regulatory guides to describe methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses (e.g., Regulatory Guide 1.168 Revision 1, *Verification, Validation, Reviews, and, Audits for Digital Computers Software Used in Safety Systems of Nuclear Power Plants*, February 2004).

important to an effective cybersecurity program for nuclear power plants. For example, RG 5.71 provides a method to aid in the categorization and identification of digital assets that must be protected from cyber attacks. It also provides a method to address and manage the potential cybersecurity risks of digital assets by applying a defensive architecture[62] and a collection of security controls. Moreover, according to RG 5.71, it is based on standards provided in NIST SP 800-53 and NIST SP 800-82,[63] among others.

Further, we determined that RG 5.71 and supplementary documents addressed 178 of 198 SP 800-53 controls, and the NRC representatives deemed the remaining 20 controls to be not applicable to their sector. Although not exactly a one-to-one match, the security controls in RG 5.71 often closely resembled the language and terminology of security controls found in SP 800-53. However, according to NRC, where applicable, the security controls in RG 5.71 have been tailored for nuclear power plants by leveraging NIST guidance in appendix I of SP 800-53 on tailoring security controls for industrial control systems. The NRC representatives provided specific reasons why the 20 controls were not applicable, as illustrated by the following examples:

- A control is not allowed because it would have a direct impact on the operational integrity of safety functions at a nuclear power plant.
- A control is not within the scope of NRC's regulatory authority.
- A control was not selected because it is not included in the NIST security control baseline for industrial control systems in NIST SP 800-53, Revision 3, Appendix I.

Table 6 provides a summary of the comparison between the nuclear sector cybersecurity guidance and federal guidance, including the controls deemed not applicable by sector representatives.

[62]According to RG 5.71, a defensive architecture establishes formal communication boundaries in which defense measures are deployed to detect, prevent, delay, mitigate, and recover from cyber attacks.

[63]NIST SP 800-82, *Guide to Industrial Control Systems Security*.

Table 6: Nuclear Sector Cybersecurity Guidance Compared with Federal Guidance

NIST control family name and number of controls	Comparison with RG 5.71 and supplementary documents
Access Control (19)	Addresses 16 of the 19 controls, and NRC staff deemed 3 controls—Remote Access, Concurrent Session Control, and User-Based Collaboration and Information Sharing—to be not applicable.
Awareness and Training (5)	Addresses all 5 controls.
Audit and Accountability (14)	Addresses all 14 controls.
Security Assessment and Authorization (6)	Addresses 5 of the 6 controls, and NRC staff deemed one control—Information System Connections—to be not applicable.
Configuration Management (9)	Addresses all 9 controls.
Contingency Planning (9)	Addresses 8 of the 9 controls, and NRC staff deemed 1 control—Alternate Processing Site—to be not applicable.
Identification and Authentication (8)	Addresses all 8 controls.
Incident Response (8)	Addresses all 8 controls.
Maintenance (6)	Addresses all 6 controls.
Media Protection (6)	Addresses all 6 controls.
Physical and Environmental Protection (19)	Addresses 17 of the 19 controls, and NRC staff deemed 2 controls—Water Damage Protection and Alternate Work Site—to be not applicable.
Planning (5)	Addresses 3 of the 5 controls, and NRC staff deemed 2 controls—Rules of Behavior and Privacy Impact Assessment—to be not applicable.
Personnel Security (8)	Addresses 7 of the 8 controls, and NRC staff deemed 1 control—Access Agreements—to be not applicable.
Risk Assessment (4)	Addresses all 4 controls.
System and Services Acquisition (14)	Addresses 11 of the 14 controls, and NRC staff deemed 3 controls—Allocation of Resources, Software Usage Restrictions, and External Information System Services—to be not applicable.
System and Communications Protection (34)	Addresses 31 of the 34 controls, and NRC staff deemed 3 controls—Network Disconnect, Honeypots, and Virtualization Techniques—to be not applicable.
System and Information Integrity (13)	Addresses 12 of the 13 controls, and NRC staff deemed 1 control—Spam Protection—to be not applicable.
Program Management (11)	Addresses 8 of the 11 controls, and NRC staff deemed 3 controls—Enterprise Architecture, Information Security Resources, and Mission/Business Process Definition—to be not applicable.

Source: GAO analysis of nuclear sector documents and interviews.

Examples of commonalities between the nuclear sector cybersecurity guidance and federal guidance, as well as the controls deemed not applicable, are described below.

Commonality: SP 800-53 recommends basic security awareness training to all information system users. RG 5.71 contains a similar control by specifying that, among other things, the licensee or applicant establish,

implement, and document training requirements for training programs to provide basic cybersecurity training for facility personnel.

Commonality: SP 800-53 recommends protection against supply chain threats by employing defense-in-breadth strategy.[64] RG 5.71 contains a similar control by specifying that the licensee or applicant protect against supply chain threats and vulnerabilities by employing the following measures: establishing trusted distribution paths, validating vendors, and requiring tamper-proof products or tamper-evident seals on acquired products.

Commonality: SP 800-53 recommends enforcing a limit of consecutive invalid access attempts by a user. RG 5.71 contains a similar control by specifying that the licensee or applicant ensure that security controls are implemented to limit the number of invalid access attempts by a user.

Not applicable: SP 800-53 recommends limiting the number of concurrent sessions for each system account. According to the NRC representatives, the concurrent session control is not applicable because it was determined that implementation of this control presents a safety risk to digital safety systems, or that systems under the scope of NRC regulations cannot support concurrent session control.

Not applicable: SP 800-53 recommends protecting information systems from damage resulting from water leakage by providing master shutoff valves that are accessible to key personnel. According to the NRC representatives, as a result of their tailoring process, the control was not selected as part of the final security control baseline in RG 5.71 because systems used at nuclear power plants are designed and built to maintain the safe operation of the plant in the event of flooding. Additionally, plant operators who are licensed by NRC are authorized to manipulate components in the facilities to control their plants.

[64]According to NIST SP 800-53, a defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

Not applicable: SP 800-53 recommends all capital planning and investment requests include the resources needed to implement the information security program and document all exceptions to this requirement. According to the NRC representatives, this security control is not necessary as licensees, by definition, must have the resources to implement their cybersecurity programs.

Conclusions

A wide variety of cybersecurity guidance is available to owners and operators of our nation's cyber-reliant critical infrastructure. Both required and voluntary guidance has been developed and issued by industry regulators, associations, and other groups that is tailored to the business needs of entities or provides methods to address unique risks or operations. While entities operating in a federal regulatory environment face enforcement mechanisms for not adhering to standards in regulatory requirements, entities not subject to regulation do not face such enforcement mechanisms, but implement such guidance to, among other things, mitigate risks, maintain profits, and meet customer expectations. In carrying out their responsibilities for coordinating efforts to protect the cyber-critical infrastructure, DHS and the other sector-specific agencies have taken steps to disseminate and promote cybersecurity guidance. However, these agencies have not identified the guidance applicable to or widely used in each of their respective critical infrastructure sectors. In addition, most sectors reviewed had not specified available guidance in their respective planning documents, in part because DHS's planning guidance did not suggest the inclusion of cybersecurity guidance. Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Greater knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets. Finally, the sector-specific cybersecurity guidance that we compared was substantially similar to guidance applicable to federal agencies.

Recommendation for Executive Action

We recommend that the Secretary of Homeland Security, in collaboration with the sector-specific agencies, sector coordinating councils, and the owners and operators of cyber-reliant critical infrastructure for the associated seven critical infrastructure sectors, determine whether it is appropriate to have key cybersecurity guidance listed in sector plans or annual plans and adjust planning guidance accordingly to suggest the inclusion of such guidance in future plans.

Agency Comments and Our Evaluation

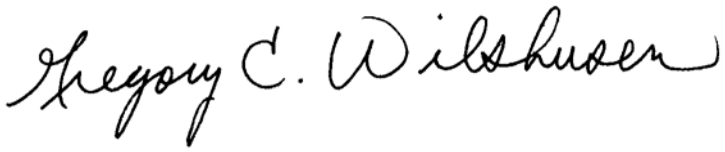
DHS provided written comments on a draft of our report (see app. III), signed by DHS's Director of Departmental GAO/OIG Liaison Office. In its comments, DHS concurred with our recommendation and stated that the department will initiate steps to implement it. In particular, DHS stated that it will work with its public and private sector partners to determine whether it is appropriate to have cybersecurity guidance drafted for each sector. DHS also indicated that the National Cyber Security Division will explore these issues with the cross-sector community.

NRC also provided written comments on a draft of our report (see app. IV), signed by the Executive Director for Operations. NRC generally agreed with the draft report.

DHS, NRC, the Department of Commerce, the Department of the Treasury, EPA, FERC, FFIEC, and HHS, also provided technical comments, which we incorporated, where appropriate. In addition, we provided relevant sections of the draft report to private sector participants. We received technical comments via e-mail from some, but not all, of these parties and incorporated their comments, where appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees; the Secretaries of Commerce, Energy, Health and Human Services, Homeland Security, and the Treasury; Administrator, Environmental Protection Agency; Executive Director, Federal Energy Regulatory Commission; Executive Secretary, Federal Financial Institutions Council; Executive Director for Operations, Nuclear Regulatory Commission; Director, Office of Management and Budget; and other interested congressional and private sector parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact Gregory Wilshusen at (202) 512-6244, or by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.



Gregory C. Wilshusen
Director, Information Security Issues

List of Requesters

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

The Honorable Yvette D. Clarke
Ranking Member
Subcommittee on Cybersecurity, Infrastructure Protection,
and Security Technologies
Committee on Homeland Security
House of Representatives

The Honorable Sheila Jackson-Lee
Ranking Member
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify (1) cybersecurity guidance for entities within selected critical infrastructure sectors, (2) the extent to which implementation of cybersecurity guidance is enforced and promoted within selected sectors, and (3) areas of commonalities and differences that exist between sectors' cybersecurity guidance and guidance applicable to federal agencies.

We focused our efforts on seven sectors: banking and finance; communications; energy (electricity and oil and natural gas); health care and public health; information technology; nuclear reactors, materials, and waste; and water. We selected these seven sectors because they are cyber-reliant or have a pervasive impact on the public's health and welfare. This determination was based on our analysis of the critical infrastructure sectors and interviews with agency officials and representatives from the sector coordinating councils. Our findings and conclusions are based on information gathered from the seven critical infrastructure sectors and are not generalizable to a larger population.

To identify cybersecurity guidance for entities within the critical infrastructure sectors, we identified and analyzed cybersecurity standards and guidance developed by federal and international standards development communities; cybersecurity policies and requirements developed by regulators for their industry; and specific industry standards, guidance, and practices developed by industry associations or groups. We interviewed sector coordinating council representatives for the seven critical infrastructure sectors to determine the cybersecurity standards used in their specific areas. On the basis of the information gathered, we developed lists of cybersecurity guidance for each sector. We provided those lists to representatives from the respective sector coordinating councils to confirm and update and to verify the applicability of the identified guidance to entities within their respective sectors.

To identify the extent to which cybersecurity guidance is enforced within the selected sectors, we gathered and analyzed related GAO reports, federal laws, regulations, and regulatory guidance to determine the various types of enforcement mechanisms that can be employed to ensure compliance. In addition, we interviewed representatives from regulatory entities: the Federal Energy Regulatory Commission, the Federal Financial Institutions Examination Council, the Nuclear Regulatory Commission, the North American Electric Reliability Corporation, and the Department of Health and Human Service's Office for Civil Rights. We also interviewed representatives from the sector coordinating councils to identify which critical infrastructure sectors have

mandatory and enforceable cybersecurity guidance. To determine efforts to identify and promote cybersecurity guidance, we collected and analyzed related federal law and policy to determine the responsibilities of the Department of Homeland Security (DHS) and the other sector-specific agencies for the seven selected sectors. In addition, we collected and analyzed the most current approved sector-specific plans, annual reports, and other related documents for the seven sectors reviewed to determine the extent of cybersecurity guidance included in the plans. Further, to determine DHS and sector-specific agency efforts related to cybersecurity standards, we interviewed sector-specific agency representatives for the seven critical infrastructure sectors to understand their programs and efforts in promoting the use of cybersecurity standards, and then collected and analyzed related supporting evidence.

To identify areas of commonalities and differences that exist between sectors' cybersecurity guidance and guidance applicable to federal agencies, we selected, analyzed, and used National Institute of Standards and Technology (NIST) Special Publication 800-37, Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* (February 2010), and NIST Special Publication 800-53, Revision 3*: Recommended Security Controls for Federal Information Systems and Organizations* (May 2010). On the basis of our analysis of these NIST documents, we identified key elements of managing cyber risk and 198 recommended security controls. To select the sector guidance to compare with guidance applicable to federal agencies, we judgmentally selected three subsectors from three different regulated sectors: the banking and finance (financial depositories); nuclear reactors, materials, and waste (reactors); and energy (bulk power) sectors. For each subsector, sector representatives identified the respective set of guidance as being widely used by entities in the sectors to meet cybersecurity-related regulatory requirements. We compared the sector cybersecurity guidance with NIST's risk management elements and recommended security controls. After our initial comparison, we interviewed relevant representatives from the regulatory entities and gathered and analyzed supplemental documentation.

We conducted this performance audit from October 2010 to December 2011 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.

Appendix II: Cybersecurity Guidance Applicable within Critical Infrastructure Sectors

This appendix contains tables listing cybersecurity guidance identified as applicable to entities within the seven critical infrastructure sectors: banking and finance; communications; energy (electricity and oil and natural gas); health care and public health; information technology; nuclear reactors, materials, and waste; and water. These lists should not be considered to include all cybersecurity guidance that may be available or used within the sector and include cybersecurity guidance that has been withdrawn by the publisher. Sector coordinating council representatives for each of the seven critical infrastructure sectors confirmed and provided additional examples, when appropriate, of the cybersecurity guidance applicable to entities within their sectors.[1] See tables 7 through 13 for the specified guidance.

Table 7: Cybersecurity Guidance Applicable to the Banking and Finance Sector

	Document title
1.	Federal Financial Institutions Examination Council (FFIEC), *IT Examination Handbook*, December 2004
2.	FFIEC, *Supplement to Authentication in an Internet Banking Environment*, June 2011
3.	Federal Reserve Board (FRB), Supervisory Letter (SR) 05-23: *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,* December 1, 2005
4.	FRB, SR Letter 05-19: *Interagency Guidance on Authentication in an Internet Banking Environment,* October 13, 2005
5.	FRB, SR Letter 04-17: FFIEC *Guidance on the use of Free and Open Source Software*, December 6, 2004
6.	FRB, SR Letter 04-14: FFIEC *Brochure with Information on Internet "Phishing,"* October 19, 2004
7.	FRB, SR Letter 02–18: *Section 312 of the USA Patriot Act—Due Diligence for Correspondent and Private Banking Accounts,* July 23, 2002
8.	FRB, SR Letter 02–6: *Information Sharing Pursuant to Section 314(b) of the USA Patriot Act,* March 14, 2002
9.	FRB, SR Letter 01–15: *Standards for Safeguarding Customer Information*, May 31, 2001
10.	FRB, SR Letter 01–11: *Identity Theft and Pretext Calling*, April 26, 2001
11.	FRB, SR Letter 00–17: *Guidance on the Risk Management of Outsourced Technology Services*, November 30, 2000
12.	FRB, SR Letter 00–04: *Outsourcing of Information and Transaction Processing,* February 29, 2000
13.	FRB, SR Letter 99–08: *Uniform Rating System for Information Technology,* March 31, 1999
14.	FRB, SR Letter 97–32: *Sound Practices Guidance for Information Security for Networks,* December 4, 1997

[1]"Cybersecurity" means the ability to protect or defend the use of cyberspace from cyber attacks. "Cyberspace" is defined as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. A "cyber attack" is further defined as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.

Document title
15. Federal Deposit Insurance Corporation (FDIC), Financial Institution Letter FIL-103-2005: FFIEC *Guidance Authentication in an Internet Banking Environment,* October 12, 2005
16. FDIC, FIL-66-2005: *Spyware – Guidance on Mitigating Risks From Spyware*, July 22, 2005
17. FDIC, FIL-64-2005: *Guidance on How Financial Institutions can Protect against Pharming Attacks*, July 18, 2005
18. FDIC, FIL-59-2005: *Identity Theft Study Supplement on "Account-Hijacking Identity Theft*," July 5, 2005
19. FDIC, FIL-46-2005: *Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process*
20. FDIC, FIL-27-2005: *Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, April 1, 2005
21. FDIC, FIL-7-2005: *Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Customer Information*, February 2, 2005
22. FDIC, FIL-132-2004: *Identity Theft Study on "Account-Hijacking" Identity Theft and Suggestions for Reducing Online Fraud,* December 14, 2004
23. FDIC, FIL-121-2004: *Computer Software Due Diligence—Guidance on Developing an Effective Software Evaluation Program to Assure Quality and Regulatory Compliance*
24. FDIC, FIL-114-2004: *Risk Management of Free and Open Source Software FFIEC Guidance*
25. FDIC, FIL-103-2004*: Interagency Informational Brochure on Internet "Phishing" Scams,* September 13, 2004
26. FDIC, FIL-84-2004: *Guidance on Instant Messaging,* July 21, 2004
27. FDIC, FIL-62-2004: *Guidance on Developing an Effective Computer Virus Protection Program,* June 7, 2004
28. FDIC, FIL-27-2004: *Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraudulent Schemes,* March 12, 2004
29. FDIC, FIL-63-2003: *Guidance on Identity Theft Response Programs,* August 13, 2003
30. FDIC, FIL-43-2003: *Guidance on Developing an Effective Software Patch Management Program,* May 29, 2003
31. FDIC, FIL–8–2002: *Wireless Networks And Customer Access,* February 1, 2002
32. FDIC, FIL–69–2001: *Authentication in an Electronic Banking Environment,* August 24, 2001
33. FDIC, FIL–68–2001: *501(b) Examination Guidance,* August 24, 2001
34. FDIC, FIL–39–2001: *Guidance on Identity Theft and Pretext Calling,* May 9, 2001
35. FDIC, FIL–22–2001: *Security Standards for Customer Information,* March 14, 2001
36. FDIC, FIL–77–2000*: Bank Technology Bulletin: Protecting Internet Domain Names,* November 9, 2000
37. FDIC, FIL–67–2000: *Security Monitoring of Computer Networks,* October 3, 2000
38. FDIC, FIL–68–99: *Risk Assessment Tools and Practices for Information System Security,* July 7, 1999
39. FDIC, FIL–98–98: *Pretext Phone Calling,* September 2, 1998
40. FDIC, FIL–131–97: *Security Risks Associated with the Internet,* December 18, 1997
41. FDIC, FIL–124–97 *Suspicious Activity Reporting,* December 5, 1997
42. FDIC, FIL–82–96: *Risks Involving Client/Server Computer Systems,* October 8, 1996
43. National Credit Union Administration (NCUA), Letter to Credit Unions 05-CU-20*: Phishing Guidance for Credit Unions and Their Members*
44. NCUA, Letter to Credit Unions 05-CU-18: *Guidance on Authentication in Internet Banking Environment,* November 2005
45. NCUA, Letter to Credit Unions 04-CU-12: *Phishing Guidance for Credit Union Members,* September 2004
46. NCUA, Letter to Credit Unions 04-CU-06: *E-Mail and Internet Related Fraudulent Schemes Guidance,* April 2004

Document title
47. NCUA, Letter to Credit Unions 04-CU-05: *Fraudulent E-Mail Schemes,* April 2004
48. NCUA, Letter to Credit Unions 03-CU-14: *Computer Software Patch Management,* September 2003
49. NCUA, Letter to Credit Unions 03-CU-12: *Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions,* August 2003
50. NCUA, Letter to Credit Unions 03-CU-08: *Weblinking: Identifying Risks & Risk Management Techniques,* April 2003
51. NCUA, Letter to Credit Unions 03-CU-03 *Wireless Technology,* February 2003
52. NCUA, Letter to Federal Credit Unions 02–FCU–11: *Tips to Safely Conduct Financial Transactions over the Internet—An NCUA Brochure for Credit Union Members,* July 2002
53. NCUA, Letter to Credit Unions 02–CU–13: *Vendor Information Systems & Technology Reviews—Summary Results,* July 2002
54. NCUA, Letter to Credit Unions 02–CU–08: *Account Aggregation Services,* April 2002
55. NCUA, Letter to Federal Credit Unions 02–FCU–04*: Weblinking Relationships,* March 2002
56. NCUA, Letter to Credit Unions 01–CU-21: *Disaster Recovery and Business Resumption Contingency Plans,* December 2001
57. NCUA, Letter to Credit Unions 01–CU–20: *Due Diligence over Third-Party Service Providers,* November 2001
58. NCUA, Letter to Credit Unions 01–CU–12: *E-Commerce Insurance Considerations,* October 2001
59. NCUA, Letter to Credit Unions 01–CU–09: *Identity Theft and Pretext Calling,* September 2001
60. NCUA, Letter to Credit Unions 01–CU–11: *Electronic Data Security Overview,* August 2001
61. NCUA, Letter to Credit Unions 01–CU–10: *Authentication in an Electronic Banking Environment,* August 2001
62. NCUA, Letter to Credit Unions 01-CU-04: *Integrating Financial Services and Emerging Technology*, March 2001
63. NCUA, Regulatory Alert 01–RA–03: *Electronic Signatures in Global and National Commerce Act (E-Sign Act),* March 2001
64. NCUA, Letter to Credit Unions 01–CU–02: *Privacy of Consumer Financial Information,* February 2001
65. NCUA, Letter to Credit Unions 00–CU–11: *Risk Management of Outsourced Technology Services (with Enclosure),* December 2000
66. NCUA, Letter to Credit Unions 00–CU–07: *NCUA's Information Systems & Technology Examination Program,* October 2000
67. NCUA, Letter to Credit Unions 00–CU–04: *Suspicious Activity Reporting* (see section on "Computer Intrusion"), July 2000
68. NCUA, Letter to Credit Unions 00–CU–02: *Identity Theft Prevention,* May 2000
69. NCUA, Regulatory Alert 99–RA–3: *Pretext Phone Calling by Account Information Brokers,* February 1999
70. NCUA, Regulatory Alert 98–RA–4: *Interagency Guidance on Electronic Financial Services and Consumer Compliance,* July 1998
71. NCUA, Letter to Credit Unions 97–CU–5: *Interagency Statement on Retail On-Line PC Banking,* April 1997
72. NCUA, Letter to Credit Unions 97–CU–1: *Automated Response System Controls,* January 1997
73. NCUA, Letter to Credit Unions 109: *Information Processing Issues,* September 1989
74. Office of the Comptroller of the Currency (OCC), Bulletin 2005-35: *Authentication in an Internet Banking Environment,* October 2005
75. OCC, Bulletin 2005-24: *Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents*, July 2005
76. OCC, Bulletin 2005-13: *Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance*, April 2005
77. OCC, Bulletin 2005-1: *Proper Disposal of Customer Information,* January 2005
78. OCC, Bulletin 2003-27: *Suspicious Activity Report-Revised Form,* June 2003
79. OCC, Advisory 2003-10*: Risk Management of Wireless Networks,* December 2003

Document title
80. OCC, Alert 2003-11: *Customer Identity Theft: E-Mail-Related Fraud Threats,* September 2003
81. OCC, Bulletin 2001–47: *Third-Party Relationships Risk Management Principles*, November 2001
82. OCC, Bulletin 2001–35: *Examination Procedures for Guidelines to Safeguard Customer Information*, July 2001
83. OCC, Alert 2001–04: *Network Security Vulnerabilities,* April 2001
84. OCC, Bulletin 2001–12: *Bank-Provided Account Aggregation Services: Guidance to Banks,* February 2001
85. OCC, Bulletin 2001–8: *Guidelines Establishing Standards for Safeguarding Customer Information,* February 2001
86. OCC, Alert 2000–9*: Protecting Internet Addresses of National Banks,* July 2000
87. OCC, Bulletin 2000–19: *Suspicious Activity Report: New SAR Form,* June 2000
88. OCC, Bulletin 2000–14: *Infrastructure Threats—Intrusion Risks: Message to Bankers and Examiners,* May 2000
89. OCC, Alert 2000–1: *Internet Security: Distributed Denial of Service Attacks,* February 2000
90. OCC, Bulletin 99–20: *Certificate Authority Guidance: Guidance for Bankers and Examiners,* May 1999
91. OCC, Bulletin 98–3: *Technology Risk Management: Guidance for Bankers and Examiners,* February 1998
92. Office of Thrift Supervision (OTS), Chief Executive Officer (CEO) Letter 97: Policy Statement on Privacy and Accuracy of Customer Information, November 3, 1998
93. OTC, CEO Letter 109: *Transactional Web Sites,* June 10, 1999
94. OTS, CEO Letter 125: *Privacy Rule,* July 6, 2000 (transmits final rule for privacy of consumer financial information)
95. OTS, CEO Letter 139: *Identity Theft and Pretext Calling*, May 4, 2001
96. OTS, CEO Letter 155*: Interagency Guidance: Privacy of Consumer Financial Information,* February 11, 2002
97. OTS, CEO Letter 193: *'Phishing' and E-mail Scams,* March 8, 2004
98. OTS, CEO Letter 214: *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,* March 30, 2005
99. OTS, CEO Letter 228: *Interagency Guidance on Authentication in an Internet Banking Environment,* October 12, 2005
100. OTS, CEO Letter 231: *Compliance Guide—Interagency Guidelines Establishing Information Security Standards,* December 14, 2005
101. OTS, CEO Letter 237: *Interagency Advisory on Influenza Pandemic Preparedness,* March 15, 2006
102. OTS, *Examination Handbook Section 341, Information Technology Risk and Controls,* October 2008
103. Payment Card Industry Data Security Standard (PCI-DSS)
104. BITS,[a] *Framework: Managing Technology Risk for IT Service Provider Relationships*
105. BITS, *Guide to Business-Critical Telecommunications Services*
106. BITS, *Guide to Business-Critical Power*
107. BITS/American Bankers Association, *Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information,* November 2006
108. U.S. Cyber Consequences Unit (CCU), *Cyber Security Check List*
109. Information System Audit and Control Association (ISACA), *Control Objectives for Information Technology* (COBIT)
110. American National Standards Institute (ANSI), *Accredited Standards Committee X9, Incorporated, Financial Industry Standards*
111. SANS Institute, *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*
112. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408:2008, *Information Technology—Security Techniques—Evaluation Criteria for IT Security*

Document title
113. ISO/IEC 24762:2008, Information Technology—Security Techniques—Guidelines for Information and Communications Technology Disaster Recovery Services
114. ISO/IEC 27000:2009, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*
115. ISO/IEC 27001:2005*, Information Technology—Security Techniques—Information Security Management Systems—Requirements*
116. ISO/IEC 27002:2005, *Information Technology—Security Techniques—Code of Practice for Information Security Management*
117. ISO/IEC 27003:2010*, Information Technology—Security Techniques—Information Security Management System Implementation Guidance*
118. ISO/IEC 27004:2009, *Information Technology—Security Techniques—Information Security Management—Measurement*
119. ISO/IEC 27005:2011, *Information Technology—Security Techniques—Information Security Risk Management*
120. ISO/IEC 27006:2007, *Information Technology—Security Techniques—Requirements for the Accreditation of Bodies Providing Audit and Certification of Information Security Management Systems*
121. ISO/IEC 27031:2011, *Information Technology—Security Techniques—Guidelines for Information and Communications Technology Readiness for Business Continuity*
122. ISO/IEC 27033 1:2009*, Information Technology—Security Techniques—Network Security*
123. National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 199: *Standards for Security Categorization of Federal Information and Information Systems,* Feb. 2004
124. NIST, FIPS Publication 200: *Minimum Security Requirements for Federal Information and Information Systems,* March 2006
125. NIST, Special Publication (SP) 800-18, Revision 1: *Guide for Developing Security Plans for Federal Information Systems,* Feb. 2006
126. NIST, SP 800-30: *Risk Management Guide for Information Technology Systems,* July 2002
127. NIST, SP 800-34, Revision 1: *Contingency Planning Guide for Federal Information Systems,* May 2010
128. NIST, SP 800-37, Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* Feb. 2010
129. NIST, SP 800-39: *Managing Information Security Risk: Organization, Mission, and Information System View,* March 2011
130. NIST, SP 800-47: *Security Guide for Interconnecting Information Technology Systems,* August 2002
131. NIST, SP 800-51, Revision 1: *Guide to Using Vulnerability Naming Schemes,* Feb. 2011
132. NIST, SP 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Aug. 2009
133. NIST, SP 800-53A, Revision 1: *Guide for Assessing the Security Controls in Federal Information Systems and Organizations,* Building Effective Security Assessment Plans, June 2010
134. NIST, SP 800-60, Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories,* August 2008
135. NIST, SP 800-70, Revision 2: *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, Feb. 2011
136. NIST, SP 800-100*: Information Security Handbook: A Guide for Managers,* Oct. 2006

Source: GAO analysis and financial services sector coordinating council.

[a]BITS is not an acronym. At one time, BITS stood for “Banking Industry Technology Secretariat.”

Table 8: Cybersecurity Guidance Applicable to the Communications Sector

	Document title
1.	Communications Security, Reliability, and Interoperability Council (CSRIC), *Cyber Security Best Practices,* March 2011
2.	Alliance for Telecommunications Industry Solutions (ATIS), Security Standards 1000007.2006 (R2011): *Generic Signaling and Control Plane Security Requirements for Evolving Networks*
3.	ATIS, 1000012.2006 (R2011): Signaling System No. 7 (SS7)—SS7 *Network and Network to Network Interface (NNI) Interconnection Security Requirements and Guidelines*
4.	ATIS, 1000019.2007: *NNI Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*
5.	ATIS, 1000024: *US Standard for Signaling Security—Security Roadmap*
6.	ATIS, 1000029.2008: *Next Generation Network (NGN) Security Requirements*
7.	ATIS, 1000030.2008: *Authentication and Authorization Requirements for Next Generation Network (NGN*)
8.	ATIS, 1000035.2009: *Next Generation Network (NGN) Identity Management (IdM) Framework*
9.	ATIS, 0300276.2008: *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*
10.	Internet Engineering Task Force (IETF), RFC 2547*: BGP/MPLS VPNs,* March 1999
11.	IETF RFC 3813: *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base* (MIB), June 2004
12.	IETF, RFC 2350: *Expectations for Computer Security Incident Response,* June 1998
13.	IETF, RFC 3227: *Guidelines for Evidence Collection and Archiving,* February 2002
14.	IETF, RFC 4942: *IPv6 Transition/Coexistence Security Considerations,* September 2007
15.	IETF, RFC 1034: *Domain Names—Concepts and Facilities,* November 1987
16.	IETF, RFC 1035: *Domain Names—Implementation and Specification,* November 1987
17.	IETF, RFC 2181: *Clarifications to the DNS Specification,* July 1997
18.	IETF, RFC 2535: *Domain Name System Security Extensions,* March 1999
19.	IETF, RFC 2870*: Root Name Server Operational Requirements,* June 2000
20.	IETF, RFC 3013: *Recommended Internet Service Provider Security Services and Procedures,* November 2000
21.	IETF, RFC 3261: *SIP: Session Initiation Protocol,* June 2002
22.	International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001: 2005: *Information Technology—Security Techniques—Information Security Management Systems—Requirements*
23.	ISO/IEC 27002: 2005: *Information Technology—Security Techniques—Code of Practice for Information Security Management*
24.	Wireless Standards, CDMA: 1XRTT, *Universal Mobile Telecommunications System*
25.	International Telecommunication Union (ITU), X.700: *Management Framework for Open Systems Interconnection for CCITT Applications*
26.	ITU, X.700-Series: *OSI Systems Management Implementors' Guide*
27.	ITU, SS7 Standards, "Securing SS7 Telecommunications Networks," *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security,* 5-6 June 2001
28.	ITU, X.800: *Security Architecture for Open Systems Interconnection for CCITT Applications*
29.	ITU, X.805: *Security Architecture for Systems Providing End-to-End Communications*
30.	ITU, X.812: *Information technology—Open Systems Interconnection—Security Frameworks for Open Systems: Access Control Framework*

Document title
31. ITU, X.815: *Information technology—Open Systems Interconnection—Security Frameworks for Open Systems: Integrity Framework*
32. ITU, X.1051: *Information technology—Security Techniques—Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002*
33. ITU, X.1250: *Baseline Capabilities for Enhanced Global Identity Management and Interoperability*
34. ITU, Y.2702: *Authentication and Authorization Requirements for NGN Release 1*
35. ITU, Y.2720: *NGN Identity Management Framework*
36. ITU, Y.2721: *NGN Identity Management Requirements and Use Cases*
37. National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) 46-3: *Data Encryption Standard,* Oct. 1999 [Withdrawn May 19, 2005]
38. NIST, FIPS 74*: Guidelines for Implementing and Using the NBS Data Encryption Standard,* April 1981 [Withdrawn May 19, 2005]
39. NIST, FIPS 81: *Data Encryption Standard Modes of Operation,* Dec. 1980 [Withdrawn May 19, 2005]
40. NIST, FIPS 140-2: *Security Requirements for Cryptographic Modules,* May 2001
41. NIST, FIPS 180-3: *Secure Hash Standard (SHS),* Oct. 2008
42. NIST, FIPS 197: *Advanced Encryption Standard,* Nov. 2001
43. NIST, Special Publication (SP) 800-12: *An Introduction to Computer Security: The NIST Handbook,* Oct. 1995
44. NIST, SP 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems,* Sept. 1996
45. NIST, SP 800-40, Version 2.0: *Creating a Patch and Vulnerability Management Program,* Nov. 2005
46. NIST, SP 800-45, Version 2: *Guidelines on Electronic Mail Security,* Feb. 2007
47. NIST, SP 800-50: *Building an Information Technology Security Awareness and Training Program,* Oct. 2003
48. NIST, SP 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* Aug. 2009
49. NIST, SP 800-54: *Border Gateway Protocol Security,* July 2007
50. NIST, SP800-57: *Recommendation for Key Management,* March 2007
51. NIST, SP 800-63, Version 1.0.2: *Electronic Authentication Guideline,* April 2006
52. NIST, SP 800-81, Revision 1: *Secure Domain Name System Deployment Guide,* April 2010
53. NIST, SP 800-83: *Guide to Malware Incident Prevention and Handling,* Nov. 2005
54. NIST, SP 800-94: *Guide to Intrusion Detection and Prevention Systems (IDPS),* Feb. 2007
55. NIST, SP 800-115: *Technical Guide to Information Security Testing and Assessment,* Sept. 2008
56. NIST, SP 800-118: *Draft Guide to Enterprise Password Management,* April 21, 2009
57. NIST, SP 800-119*: Guidelines for the Secure Deployment of IPv6*, Dec. 2010
58. NIST, SP 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010
59. National Security Agency (NSA), *Security Configuration Guides*
60. NSA, *VOIP and IP Telephony Security Configuration Guides*
61. CableLabs, DOCSIS 2.0®: *Baseline Privacy Plus Interface Specification* (CM-SP-BPI+-C01-081104), November 4, 2008
62. CableLabs, DOCSIS 3.0® : Security Specification (CM-SP-SECv3.0-I13-100611), June 11, 2010
63. CableLabs, PacketCable™: Security 2.0 Technical Report (PKT-TR-SEC-V05-080425)
64. CableLabs, PacketCable™: Security Specification (PKT-SP-SEC1.5-I03-090624)

Document title
65. CableLabs, PacketCable™ IMS Delta Specifications: 3G Security; Access Security for IP-Based Services Specification 3GPP TS 33.203 (PKT-SP-33.203-I05-090528)
66. Information Security Forum (ISF), Security Audit of Networks
67. ISF, 2007 Standard of Good Practice for Information Security
68. National Security Telecommunications Advisory Committee (NSTAC), ISP Working Group on Border Gateway Protocol Interoperability Testing[a]
69. NSTAC, Network Security Information Exchange
70. NSTAC, Operations, Administration, Maintenance and Provisioning Security Requirements for Public Telecommunications Network
71. Center For Internet Security (CIS), Benchmarks
72. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1
73. Liberty Alliance Project, Privacy and Security Best Practices, Version 2.0
74. SANS Institute, Vulnerability Management: Tools, Challenges and Best Practices
75. Telecordia GR-815, Generic Requirements for Network Element/Network System (NE/NS) Security, March 2002
76. Network Reliability and Interoperability Council (NRIC), Cybersecurity Best Practices

Source: GAO analysis and communications sector coordinating council.

[a]The title of this document was provided by SCC representatives. GAO was not able to confirm the existence of the document itself.

Table 9: Cybersecurity Guidance Applicable to the Energy Sector

Document title
Electricity subsector
North American Electric Reliability Corporation (NERC) mandatory cyber security standards 002 through 009 (where applicable)
1. NERC, Critical Infrastructure Protection (CIP) Cyber Security Standard 002*: Critical Cyber Asset Identification (CIP-002-3)*
2. NERC, CIP Cyber Security Standard 003: *Security Management Controls (CIP-003-3)*
3. NERC, CIP Cyber Security Standard 004*: Personnel and Training (CIP-004-3)*
4. NERC, CIP Cyber Security Standard 005: *Electronic Security Perimeter(s) (CIP-005-3)*
5. NERC, CIP Cyber Security Standard 006*: Physical Security of Critical Cyber Assets* (CIP-006-3)
6. NERC, CIP Cyber Security Standard 007: *Systems Security Management* (CIP-007-3)
7. NERC, CIP Cyber Security Standard 008*: Incident Reporting and Response Planning* (CIP-008-3)
8. NERC, CIP Cyber Security Standard 009: *Recovery Plans for Critical Cyber Assets* (CIP-009-3)
NERC, security guidelines for the electricity sector
9. NERC, *Security Guidelines for the Electricity Sector*, Version 1.0, June 14, 2002[a]
10. NERC, *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets,* Version 1.0, June 17, 2010[b]
11. NERC, *Security Guideline for the Electricity Sector: Identifying Critical Assets,* Version 1.0 (September 17, 2009)
12. NERC, *Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Planning,* Version 1.0, May 2, 2007
13. NERC, *Security Guidelines for the Electricity Sector: Continuity of Operations,* Version 2.0, May 2007

Document title
14. NERC, *Security Guidelines for the Electricity Sector: Physical Security,* Version 2.0, May 2007
15. NERC, *Security Guidelines for the Electricity Sector: Control System–Business Network Electronic Connectivity,* Version 1.0, May 3, 2005
16. NERC, *Security Guidelines for the Electricity Sector: Patch Management for Control Systems,* Version 1.0, May 3, 2005
17. NERC, *Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems,* Version 1.0, June 10, 2003
18. NERC, *Security Guidelines for the Electricity Sector: Physical Response,* Version 3.0, November 1, 2005
19. NERC, *Security Guidelines for the Electricity Sector: Physical Security–Substations,* Version 1.0, October 15, 2004
20. NERC, *Security Guideline for the Electricity Sector: Threat and Incident Reporting,* Version 2.0, April 1, 2008
21. NERC, *Threat Alert System and Cyber Response Guidelines for the Electricity Sector, Definitions of Cyber Threat Alert Levels, A Model for Developing Organization Specific Cyber Threat Alert Level Response Plans*, Version 2.0, October 8, 2002
Other standards
22. International Electrotechnical Commission (IEC), Technical Specification (TS) 62351-1: *Power Systems Management and Associated Information Exchange—Data and Communications Security,* Parts 1-7
23. IEC 61850-90-5 for PMUs[c]
24. IEC TC65C, which is standardizing the ISA SP99 Security Standards (IEC 62443)[c]
25. Institute of Electrical and Electronic Engineers (IEEE) 802.11i: *Security for Wireless*
26. IEEE 1686-2007: *Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
27. IEEE 1588-2008: *Standard for a Precision Clock Synchronization Protocol for Network Measurement and Control Systems*
28. IEEE 1547.3-2007: *Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected With Electric Power Systems*
29. IEEE 1815-2010: *Electric Power Systems Communications—Distributed Network Protocol (DNP3)*
30. IEEE 1815.1: *Mapping between DNP3 and IEC 61850 with Security (pending)*[c]
31. IEEE P37.238*: PMUs with Security*[c]
32. IEEE 1703: ANSI C12.22, which includes the security for AMI communications[c]
33. International Organization for Standardization (ISO) 27010 series
34. ISO/IEC 21827:2008, Information Technology—Security Techniques—Systems Security Engineering—Capability Maturity Model® (SSE-CMM®)
35. NIST, Interagency Report (IR) 7628*, Guidelines for Smart Grid Cyber Security,* August 2010
Oil and natural gas subsector
36. American Chemical Council, Guidance Document*: Guidance for Addressing Cyber Security in the Chemical Industry,* November 2009
37. American Petroleum Institute (API), *Security Guidelines for the Petroleum Industry,* Third Edition, April 2005
38. API Standard 1164, *Pipeline SCADA Security,* June 2009
39. API & National Petrochemical & Refiners Association (NPRA), *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries,* Second Edition
40. API, *Security for Offshore Oil and Natural Gas Operations: API Recommended Practice 70*, First Edition, March 2003, reaffirmed, September 2010
41. API, *Security for Worldwide Offshore Oil and Natural Gas Operations: API Recommended Practice 70I*, First Edition , May 2004
42. API, *Standard for Third Party Network Connectivity,* November 2007

Document title
43. Interstate Natural Gas Association of America (INGAA), Control Systems Cyber Security Working Group, *Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry,* January 31, 2011
44. American Gas Association (AGA) Report 12, *Cryptographic Protection of SCADA Communications: Part 1: Background, Policies and Test Plan* (AGA 12, Part 1), March 14, 2006
45. AGA and Interstate Natural Gas Association of America (INGAA), *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*, May 2008
46. American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-2010, (IEC 62264-1 Mod) *Enterprise-Control System Integration Part 1: Models and Terminology*, approved May 13, 2010
47. ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems: Part I: Terminology, Concepts, and Models,* Oct. 2007
48. ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program,* Jan. 13, 2009
49. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2005, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*
50. ISO/IEC 27002:2005, *Information Technology—Security Techniques—Code of Practice for Information Security Management*[d]
51. Department of Homeland Security (DHS) Control Systems Security Program, *Cyber Security Evaluation Tool (CSET*)
52. DHS, *National Cyber Security Division, Control Systems Security Program, Catalog of Control Systems Security: Recommendations for Standards Developers,* April 2011
53. DHS*, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency,* 2009
54. DHS, *Cyber Security Procurement Language for Control Systems,* Sept. 2009
55. DHS *Transportation Security Administration (TSA), Pipeline Security Guidelines*, Dec. 2010.
56. DOE/The President's Critical Infrastructure Protection Board, 21 *Steps to Improve Cyber Security of SCADA Networks*
57. National Institute of Standards and Technology (NIST), SP 800-16 Revision 1, *Draft Information Security Training Requirements: A Role- and Performance-Based Model,* Mar. 20, 2009
58. NIST, SP 800-36*: Guide to Selecting Information Technology Security Products,* Oct. 2003
59. NIST, SP 800-48 Rev 1: *Guide to Securing Legacy IEEE 802.11 Wireless Networks,* July 2008
60. NIST, SP 800-50: *Building an Information Technology Security Awareness and Training Program,* Oct. 2003
61. NIST, SP 800-52: *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,* June 2005
62. NIST, SP 800-53 Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
63. NIST, SP 800-53A Revision 1*: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* July 2010
64. NIST, SP 800-61 Revision 1: *Computer Security Incident Handling Guide,* Mar. 2008
65. NIST, SP 800-63, Version 1.0.2: *Electronic Authentication Guideline,* April 2006
66. NIST, SP 800-73-3: *Interfaces for Personal Identity Verification,* February 2010
67. NIST, SP 800-76-1: *Biometric Data Specification for Personal Identity Verification,* Jan. 2007
68. NIST, SP 800-82: *Guide to Industrial Control Systems (ICS) Security,* June 2011
69. NIST, SP 800-83: *Guide to Malware Incident Prevention and Handling,* Nov. 2005
70. NIST, SP 800-86: *Guide to Integrating Forensic Techniques into Incident Response,* Aug. 2006

Document title
71. NIST, SP800-97: *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,* Feb. 2007
72. The White House, *The National Strategy to Secure Cyberspace,* Feb. 2003

Source: GAO analysis and the energy sector coordinating councils for electricity and oil and natural gas.

[a]NERC has not updated this document, but instead created stand-alone documents that address specific topics, many of which are in the midst of being reviewed and updated.

[b]This guide is intended to assist entities in implementing the mandatory standard (CIP-002).

[c]The title of this document was provided by SCC representatives. GAO was not able to confirm the existence of the document itself.

[d]ISO/IEC 27002 was formerly known as ISO/IEC 17799.

Table 10: Cybersecurity Guidance Applicable to the Health Care and Public Health Sector

Document title
1. ASTM International,[a] Standard E1869-04, 2010, Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
2. ASTM Standard E1985-98, 2005, Guide for User Authentication and Authorization
3. ASTM Standard E1986-09, Guide for Information Access Privileges to Health Information
4. ASTM Standard E1987-98, Guide for Individual Rights Regarding Health Information [withdrawn 2007 – no replacement]
5. ASTM Standard E2085-00a, Guide on Security Framework for Healthcare Information [withdrawn 2009 – no replacement]
6. ASTM Standard E2086-00, Guide for Internet and Intranet Healthcare Security [withdrawn 2009 – no replacement]
7. ASTM Standard E2595-07, Guide for Privilege Management Infrastructure
8. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2005, Information Technology—Security Techniques—Information Security Management Systems—Requirements
9. ISO/IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management
10. ISO 27799:2008, Health Informatics: Information Security Management in Health Using ISO/IEC 27002
11. ISO 15408: Common Criteria for Information Technology Security Evaluation
12. ISO/IEC 27032, Information Technology—Security Techniques—Guidelines for Cybersecurity (FCD)
13. National Institute of Standards and Technology (NIST), SP 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations, August 2009
14. NIST Special Publication 800-53A, Revision 1: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, June 2010
15. NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
16. COBIT 4.1 (Published Version), COBIT 5—Release 2012
17. PCI DSS, Version 2.0 (Oct. 2010)—PCI Data Security Standard
18. FTC, Red Flags Rule (November 2007), Federal Trade Commission—Identify Theft

Document title
19. HI TRUST, Common Security Framework
20. The Web Services-Interoperability Organization, Security Challenges, Threats and Countermeasures, Version 1.0, November 2010

Source: GAO analysis and health care and public health sector coordinating council

[a]ASTM International, known until 2001 as the American Society for Testing and Materials (ASTM), is an international standards organization that develops and publishes voluntary consensus technical standards for a wide range of materials, products, systems, and services.

Table 11: Cybersecurity Guidance Applicable to the Information Technology Sector

Document title
1. Alliance for Telecommunications Industry Solutions (ATIS), ATIS 0300074.2009, *Guidelines and Requirements for Security Management Systems,* March 2009
2. ATIS T1.3GPP.33.120V400-2002, *Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives,* March 2001
3. European Telecommunications Standards Institute (ETSI), TS 102 165-1, *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN): Method and Protocols; Part 1: Method and Proforma for Threat, Risk and Vulnerability Analysis,* March 2011
4. ETSI: TS 102 165-2, TISPAN; *Methods and Protocols, Part 2: Protocol Framework Definition; Security Counter Measures,* February 2007
5. ETSI: TS 102 227, *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception,* May 2004
6. ETSI: TS 102 419, *TISPAN; Security Analysis of IPv6 Application in Telecommunications Standards,* April 2005
7. ETSI: TS 187 001, *TISPAN; NGN SECurity (SEC); Requirements*, March 2006
8. Internet Engineering Task Force (IETF), IETF 3013, *Recommended Internet Service Provider Security Services and Procedures,* November 2000
9. IETF RFC 4778, *Operational Security: Current Practices in Internet Service Provider Environments,* January 2007
10. IETF RFC 2196*, Site Security Handbook,* September 1997
11. IETF RFC 2504, *Users' Security Handbook,* February 1999
12. IETF RFC 3365, *Strong Security Requirements for Internet Engineering Task Force Standard Protocols*, August 2002
13. IETF RFC 3631, *Security Mechanisms for the Internet,* December 2003
14. IETF RFC 3871, *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure,* September 2004
15. IETF RFC 5637, *Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6,*[a] September 2009
16. IETF RFC 5765, *Security Issues and Solutions in Peer-to-Peer Systems for Realtime Communications*, February 2010
17. IETF: WG RFC 4190, *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony,* Nov. 2005
18. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2005, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*
19. ISO/IEC 27002:2005, *Information Technology—Security Techniques—Code of Practice for Information Security Management*
20. ISO/IEC FCD 27032, *Information Technology—Security Techniques—Guidelines for Cybersecurity*
21. ISO/IEC 27033-1:2009, *Information Technology—Security Techniques—Network Security—Part 1: Overview and Concepts*

Document title
22. ISO/IEC FCD 27033-2.2, *Information Technology—Security Techniques—Network Security—Part 2: Guidelines for the Design and Implementation of Network Security*
23. ISO/IEC 27033-3:2010, *Information Technology—Security Techniques—Network Security—Part 3: Reference Networking Scenarios—Threats, Design Techniques, and Control Issues*
24. Internet Security Alliance, *Financial Management of Cyber Risk: An Implementation Framework for CFOs*
25. Internet Security Alliance*, Social Contract 2.0: A 21st Century Program for Effective Cyber Security*
26. Internet Security Alliance, *The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress, 2008*
27. Internet Security Alliance, *Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask,* 2008
28. Internet Security Alliance, *Navigating Compliance and Security for Unified Communications,* 2009
29. Internet Security Alliance, *Common Sense Guide for Home & Individual Users,* 2003
30. Internet Security Alliance, *Common Sense Guide to Cyber Security for Small Businesses,* 2004
31. Internet Security Alliance, *Common Sense Guide for Senior Managers,* 2002
32. International Telecommunications Union-Telecommunication Standardization Sector (ITU-T): *Y.2720, NGN [Next Generation Networks] Identity Management Framework*
33. ITU-T, *Security in Telecommunications and Information Technology: An overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications,* September 2009
34. ITU-T, X.1205: *Overview of Cybersecurity*
35. ITU-T: E.408, *Telecommunication Networks Security Requirements*
36. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12: *An Introduction to Computer Security: The NIST Handbook,* October 1995
37. NIST, SP 800-30: *Risk Management Guide for Information Technology Systems,* July 2002
38. NIST, SP 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organization,* August 2009
39. NIST, SP 800-53A, Revision 1: *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* June 2010
40. NIST, SP 800-50: *Building an Information Technology Security Awareness and Training Program,* October 2003

Source: GAO analysis and information technology sector coordinating council.

Note: These are illustrative examples of cybersecurity guidance used in the sector.

[a]IPv6 is Internet Protocol Version 6.

Table 12: Cybersecurity Guidance Applicable to the Nuclear Reactors, Materials, and Waste Sector

Document title
1. Nuclear Regulatory Commission (NRC), Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities*, January 2010
2. Nuclear Energy Institute (NEI) 08-09, Revision 6: *Cyber Security Plan for Nuclear Power Reactors,* April 2010
3. NEI 10-04, Revision 1: *Scope of Systems for the NRC Cyber Security 10 CFR §73.54 and FERC Order 706-B Compliance,* June 2011
4. NEI 10-08: *Cyber Security Rule Implementation Review Program* (Under development)
5. NEI 10-09: *Addressing Cyber Security Controls for Nuclear Power Reactors* (Under development)
6. Electric Power Research Institute (EPRI) technical report 1019187, *Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems,* October 29, 2010
7. NRC, Regulatory Guide 1.152, Revision 2: *Criteria for Use of Computers in Safety Systems of Nuclear Power Plant,* January 2006
8. NRC, Regulatory Guide 1.168, Revision 1: *Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,* February 2004
9. NRC, Regulatory Guide 1.169: *Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,* September 1997
10. Draft NRC Regulatory Guide DG-5019, Revision 1: *Reporting and Recording Safeguards Events*, January 2011
11. NRC, NUREG/CR-6847: *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*
12. NRC, NUREG-800, Branch Technical Position 7-14, Revision 5: *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,* March 2007
13. NIST, SP 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
14. NIST, SP 800-82: *Guide to Industrial Control Systems (ICS) Security,* June 2011
15. NIST, SP 800-86: *Guide to Integrating Forensic Techniques into Incident Response,* August 2006
16. DHS, *Catalog of Control Systems Security: Recommendations for Standards Developers,* April 2011
17. NERC CIP 002-2 through CIP 009-2, May 6, 2009
18. IEEE Standard 7-4.3.2-2010, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,* August 2, 2010

Source: GAO analysis and the nuclear reactors, materials, and waste sector coordinating council.

Table 13: Cybersecurity Guidance Applicable to the Water Sector

	Document title
1.	American National Standards Institute (ANSI)/The Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA-99.00.01-2007: *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models,* Oct. 2007
2.	ANSI/ISA-99.02.01-2009*: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program,* January 13, 2009
3.	ANSI/American Society of Mechanical Engineers (ASME-ITI)/American Water Works Associations (AWWA), J100-10: *Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems,* 1st edition, July 1, 2010
4.	ANSI/AWWA G430-09: *Security Practices for Operations and Management,* 1st edition, May 1, 2009
5.	AWWA M2: *Instrumentation and Control,* 3RD edition, 2001 (currently under revision)
6.	Department of Homeland Security (DHS), Cyber Security Evaluation Tool (CSET)
7.	DHS, *Cyber Security Procurement Language for Control Systems,* September 2009
8.	DHS, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers,* June 2010 [updated April 2011]
9.	EPA Security Product Guides: *Anti-Virus and Pest Eradication Software; Firewalls; and Network Intrusion Hardware/Software*
10.	International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2005: *Information technology—Security Techniques—Information Security Management Systems—Requirements*
11.	ISO/IEC 27002:2005: *Information technology—Security Techniques—Code of Practice for Information Security Management*
12.	National Institute of Standards and Technology (NIST), Special Publication (SP) NIST SP 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
13.	NIST, SP 800-82: *Guide to Industrial Control Systems (ICS) Security,* June 2011
14.	North American Electric Reliability Corporation (NERC,) Critical Infrastructure Protection (CIP) Cyber Security Standards 002 through 009
15.	Awwa Research Foundation (AwwaRF) and Sandia National Laboratories, *The Environmental Protection Agency, Risk Assessment Methodology–Water* (RAM-W), December 2001
16.	SANS Institute, *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*
17.	SANS Institute, *Vulnerability Management: Tools, Challenges and Best Practices*
18.	EPA Vulnerability Self-Assessment Tool (VSAT) 5.0 for water and wastewater utilities, September 2010

Source: GAO analysis and the water sector coordinating council.

Appendix III: Comments from the Department of Homeland Security

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

Homeland Security

November 23, 2011

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

Re: Draft Report GAO-12-92, "CRITICAL INFRASTRUCTURE PROTECTION: Cybersecurity Guidance Available, but More Can be Done to Promote Its Use"

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) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive acknowledgment of actions DHS has taken to coordinate efforts to protect the cyber critical infrastructure and to disseminate and promote cybersecurity guidance. For example, the report recognizes that DHS promotes standards and practices from a cross-sector perspective, and engages frequently with several other government agencies, organizations and international bodies to provide sectors with resources on security standards. In addition, the report recognizes that DHS has issued recommended practices to reduce cybersecurity risks to industrial control systems within and across all critical infrastructure sectors. DHS's guidance for preparing sector-specific critical infrastructure plans includes outlining each sector's cyber protection and resilience strategies.

Under Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," DHS and its public and private sector partners jointly developed and are implementing the National Infrastructure Protection Plan (NIPP). The NIPP and its complementary Sector-Specific Plans provide a consistent, unifying structure for integrating current and future critical infrastructure protection and resilience efforts. To address cyber risk, DHS's National Protection and Programs Directorate, National Cyber Security Division (NCSD) executes its NIPP responsibilities serving as the Sector-Specific Agency for the Information Technology Sector and providing cybersecurity knowledge and expertise to the other 17 critical infrastructure sectors defined in the NIPP. Although DHS engages in numerous public-private sector support activities, the Department does not currently have the authority to establish regulatory standards.

The draft report contained one recommendation directed at DHS, with which the Department concurs and has already initiated steps to implement. Specifically, GAO recommended that:

Recommendation: The Secretary of Homeland Security, in collaboration with the sector-specific agencies, sector coordinating councils, and the owners and operators of cyber-reliant critical infrastructure for the associated seven critical infrastructure sectors, determine whether it is appropriate to have key cybersecurity guidance listed in sector plans and/or annual plans and adjust planning guidance accordingly to suggest the inclusion of such guidance in future plans.

Response: Concur. DHS will work with its public and private sector partners under the auspices of the Critical Infrastructure Partnership Advisory Council, and in accordance with the NIPP Partnership Framework, to determine whether it is appropriate to have cybersecurity guidance drafted for each sector. It is imperative that DHS work with the respective Sector Coordinating Councils (SCCs) to determine what cybersecurity guidance may be appropriate in each sector and to collaborate on the format(s) of that guidance. The SCCs are self-organized, self-run, and self-governed. Specific membership varies from sector to sector, reflecting the unique composition of each sector; the Councils are encouraged to participate in efforts to develop voluntary consensus standards to ensure that sector perspectives are included in standards that affect critical infrastructure protection. NCSD will explore these issues with the cross-sector community.

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments were previously provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

Appendix IV: Comments from the Nuclear Regulatory Commission

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

November 25, 2011

Mr. Michael Gilmore, Assistant Director
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Gilmore:

The U.S. Nuclear Regulatory Commission (NRC) appreciates the opportunity to provide comments on the draft report titled, "Critical Infrastructure Protection - Cybersecurity Guidance Available, but More Can Be Done to Promote Its Use" (GAO-12-92). In general, the NRC agrees with the draft report. The NRC's comments are enclosed for your consideration, and inclusion in the final report as noted in your e-mail of October 28, 2011.

Please direct any questions or concerns that you may have regarding NRC's comments to Mr. Jesse Arildsen, at (301) 415-1785 or email to Jesse.Arildsen@nrc.gov.

Sincerely,

R. W. Borchardt
Executive Director
for Operations

Enclosure:
As stated

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Michael W. Gilmore (Assistant Director), Lon C. Chin, Wilfred B. Holloway, Franklin D. Jackson, Barbarol J. James, Lee McCracken, Krzysztof Pasternak, and John A. Spence made key contributions to this report.

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 website (www.gao.gov). Each weekday afternoon, GAO posts on its website 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 website, 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.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: 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