Cybersecurity: Critical Infrastructure Authoritative Reports and Resources

Rita Tehan
Information Research Specialist

December 6, 2016

Congressional Research Service
7-5700
www.crs.gov
R44410

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Critical infrastructure is defined in the USA PATRIOT Act (P.L. 107-56, §1016(e)) as "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

Presidential Decision Directive 63, or PDD-63, identified activities whose critical infrastructures should be protected: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production; and storage. In addition, the PDD identified four activities in which the federal government controls the critical infrastructure: (1) internal security and federal law enforcement; (2) foreign intelligence; (3) foreign affairs; and (4) national defense.

In February 2013, the Obama Administration issued PPD-21, Critical Infrastructure Security and Resilience, which superseded HSPD-7 issued during the George W. Bush Administration. PPD-21 made no major changes in policy, roles and responsibilities, or programs, but did order an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability. PPD-21 also called for an update of the National Infrastructure Protection Plan, and a new Research and Development Plan for Critical Infrastructure, to be updated every four years.

This report serves as a starting point for congressional staff assigned to cover cybersecurity issues as they relate to critical infrastructure. Much is written about protecting U.S. critical infrastructure, and this CRS report directs the reader to authoritative sources that address many of the most prominent issues. The annotated descriptions of these sources are listed in reverse chronological order with an emphasis on material published in the past several years. The report includes resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources.

- **Table 1** contains overview reports and resources
- **Table 2** lists energy resources, including electrical grid, Smart Grid, SCADA, and Industrial Control Systems
- **Table 3** presents financial industry resources, including banks, insurance, SEC guidance, FFIEC, FDIC, FSOC, and IRS
- **Table 4** contains health, including Healthcare.gov, health insurance, Medicaid, and medical devices
- **Table 5** contains telecommunications and communications, including wired, wireless, Internet service providers, GPS, undersea cables, and public safety broadband networks
- **Table 6** features transportation, including Coast Guard, air traffic control, ports and maritime, and automobiles

The following CRS reports comprise a series that compiles authoritative reports and resources on these cybersecurity topics:

- CRS Report R44405, *Cybersecurity: Overview Reports and Links to Government, News, and Related Resources*, by Rita Tehan

- CRS Report R44406, *Cybersecurity: Education, Training, and R&D Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44408, *Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan
- CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan
- CRS Report R44417, *Cybersecurity: State, Local, and International Authoritative Reports and Resources*, by Rita Tehan

For access to additional CRS reports and other resources, see the *Science & Technology: Science for Security and Homeland Security & Immigration: Cybersecurity Issue Pages* at http://www.crs.gov.

Contents

Tables

Contacts

Introduction

Critical infrastructure is defined in the USA PATRIOT Act (P.L. 107-56, §1016(e)) as "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."[1]

Presidential Decision Directive 63 (or PDD-63) identified activities whose critical infrastructures should be protected:

- information and communications;
- banking and finance;
- water supply;
- aviation, highways, mass transit, pipelines, rail, and waterborne commerce;
- emergency and law enforcement services;
- emergency, fire, and continuity of government services;
- public health services;
- electric power, oil and gas production; and
- storage.

In addition, PDD-63 identified four activities in which the federal government controls the critical infrastructure: (1) internal security and federal law enforcement; (2) foreign intelligence; (3) foreign affairs; and (4) national defense.

In February 2013, the Obama Administration issued PPD-21, the Critical Infrastructure Security and Resilience,[2] which superseded HSPD-7 issued during the George W. Bush Administration. PPD-21 made no major changes in policy, roles and responsibilities, or programs, but did order an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability. PPD-21 also called for an update of the National Infrastructure Protection Plan and a new Research and Development Plan for Critical Infrastructure, to be updated every four years.

This report serves as a starting point for congressional staff assigned to cover cybersecurity issues as they relate to critical infrastructure. Much is written about protecting U.S. critical infrastructure, and this CRS report directs the reader to authoritative sources that address many of the most prominent issues. The annotated descriptions of these sources are listed in reverse

[1] See P.L. 107-56, §1016(e). Homeland Security Presidential Directive Number 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, released December 17, 2003, went further to describe the level of impact the loss of an asset must have to warrant considering the asset as "critical." This included causing catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction; impairing federal agencies' abilities to perform essential missions or ensure the public's health and safety; undermining state and local government capacities to maintain order and deliver minimum essential public services; damaging the private sector's capability to ensure the orderly functioning of the economy; having a negative effect on the economy through cascading disruption of other infrastructures; or undermining the public's morale and confidence in our national economic and political institutions. HSPD-7 has since been superseded by PDD-21.

[2] See Critical Infrastructure Security and Resilience, The White House, February 12, 2013 at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

chronological order with an emphasis on material published in the last several years. This report includes resources and studies from government agencies (federal, state, local, and international), think tanks, academic institutions, news organizations, and other sources related to the following sectors:

- **Table 1**, overview reports and resources;
- **Table 2**, energy, including electrical grid, smart grid, SCADA, and industrial control systems;
- **Table 3**, financial industry, including banks, insurance, SEC guidance, FFIEC, FDIC, FSOC, and IRS;
- **Table 4**, health, including Healthcare.gov, health insurance, Medicaid, and medical devices;

  Table 5, telecommunications and communications, including wired, wireless, Internet service providers, GPS, undersea cables, and public safety broadband network; and
- **Table 6**, transportation, including Coast Guard, air traffic control, ports and maritime, and automobiles.

Table 1. Overview Reports and Resources

Title	Source	Date	Notes
Critical Infrastructure Sectors (list)	Department of Homeland Security (DHS)	Continuously Updated	There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation Systems; and water and wastewater systems.
Daily Open Source Infrastructure Report	DHS	Continuously Updated	The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. The Daily Report is collected each business day as a summary of open-source published information concerning significant critical infrastructure issues. Each report is divided by the critical-infrastructure sectors and key assets defined in the National Infrastructure Protection Plan.
Cyber Infrastructure Protection	Homeland Security Digital Library (HSDL)	Continuously Updated	General resources for cyber infrastructure protection, grouped by audits and investigations, CRS reports, DOD reports, executive branch, exercise reports, hearings, international perspective, research and analysis, thesis, and websites.
National Council of ISACs	Information Sharing and Analysis Centers (ISAC)	Continuously Updated	The mission of the National Council of ISACs (NCI) is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors.
ICS-CERT Monitor Newsletters	Industrial Control Systems Cyber Emergency Response Team (ICS/CERT) Monitor	Continuously Updated	ICS-CERT publishes the Monitor Newsletter when an adequate amount of pertinent information has been collected. The newsletter is a service to personnel actively engaged in the protection of critical infrastructure assets.

Title	Source	Date	Notes
Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments but Additional Improvements are Needed	GAO	July 12, 2016	This testimony summarizes past GAO findings on progress made and improvements needed in DHS's vulnerability assessments, such as addressing potential duplication and gaps in these efforts. (21 pages)
Incident Response Activity (November-December 2015)	ICS/CERT	January 19, 2016	U.S. critical infrastructure systems experienced a 20% increase in attempted cybersecurity breaches in FY2015, ICS-CERT responded to 295 cybersecurity incidents involving critical infrastructure, compared with 245 in fiscal 2014. (10 pages)
Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts	Government Accountability Office (GAO)	September 15, 2014	DHS used 10 different assessment tools and methods from FY2011 through FY2013 to assess critical infrastructure vulnerabilities. Four of the 10 assessments did not include cybersecurity. The differences in the assessment tools and methods mean DHS is not positioned to integrate its findings in identifying priorities. (82 pages)
Actions to Strengthen Cybersecurity and Protect Critical IT Systems	Office of Personnel Management (OPM)	June 24, 2015	OPM lists 15 new steps and 23 ongoing actions to secure its computer networks. The agency plans to ask for additional funds for its IT budget next fiscal year. (8 pages)
Critical Infrastructure: Security Preparedness and Maturity	Unisys and the Ponemon Institute	July 2014	Unisys and the Ponemon Institute surveyed nearly 600 IT security executives of utility, energy, and manufacturing organizations. Overall, the report finds organizations are simply not prepared to deal with advanced cyber threats. Only half of companies have actually deployed IT security programs and, according to the survey, the top threat actually stems from negligent insiders. (34 pages)
Sector Risks Snapshots	DHS	May 2014	DHS's snapshots provide an introduction to the diverse array of critical infrastructure sectors, touching on some of the key threats and hazards concerning these sectors and highlighting the common, first-order dependencies and interdependencies between sectors. (52 pages)

Title	Source	Date	Notes
Notice of Completion of Notification of Cyber-Dependent Infrastructure and Process for Requesting Reconsideration of Determinations of Cyber Criticality	DHS Programs Directorate	April 17, 2014	The Secretary of DHS has been directed to identify critical infrastructure in which a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In addition to identifying such infrastructure, the Secretary must confidentially notify the infrastructure's owners and operators and establish a mechanism through which entities can request reconsideration of that identification, whether inclusion of or exclusion from the list. The notice informs owners and operators of critical infrastructure that the confidential notification process is complete and describes the process for requesting reconsideration. (3 pages)
Framework for Improving Critical Infrastructure Cybersecurity	National Institute of Standards and Technology (NIST)	February 12, 2014	The voluntary framework consists of customizable cybersecurity standards that can be adapted by various sectors and both large and small organizations. To encourage the private sector to fully adopt this framework, DHS launched the Critical Infrastructure Cyber Community (C^3)—or C-cubed—Voluntary Program. The C^3 program gives companies that provide critical services such as cell phones, email, banking, and energy and state and local governments direct access to DHS cybersecurity experts within DHS who have knowledge about specific threats, ways to counter those threats, and how, over the long term, to design and build systems that are less vulnerable to cyber threats. (41 pages)
ITI Recommendations to the Department of Homeland Security Regarding its Work Developing a Voluntary Program Under Executive Order 163636, "Improving Critical Infrastructure Cybersecurity."	Information Technology Industry Council (ITI)	February 11, 2014	ITI released a set of recommendations that suggest DHS prioritize outreach to raise awareness of the framework and the program as resources; carefully determine how "success" is to be demonstrated; de-emphasize the current focus on incentives; and partner with industry on all aspects of the program moving forward. (3 pages)
The Federal Government's Track Record on Cybersecurity and Critical Infrastructure	Senate Homeland Security and Governmental Affairs Committee (Minority Staff)	February 4, 2014	Since 2006, the federal government has spent at least $65 billion on securing its computers and networks, according to an estimate by the Congressional Research Service (CRS). NIST, the government's official body for setting cybersecurity standards, has produced thousands of pages of precise guidance on every significant aspect of IT security. And yet the Senate report found that agencies—even those with responsibilities for critical infrastructure or vast repositories of sensitive data—continue to leave themselves vulnerable, often by failing to take the most basic steps toward securing their systems and information. (19 pages)

Title	Source	Date	Notes
Computer Security Incident Coordination (CSIC): Providing Timely Cyber Incident Response	NIST	June 28, 2013	NIST is seeking information relating to CSIC as part of the research needed to compile a new supplemental publication to help computer security incident response teams (CSIRTs) coordinate effectively when responding to computer-security incidents. The NIST special publication will identify technical standards, methodologies, procedures, and processes that facilitate prompt and effective response. (3 pages)
Cyber Infrastructure Protection: Volume II	U.S. Army War College Press	May 2013	The book addresses such questions as how serious is the cyber threat? What technical and policy-based approaches are best suited to securing telecommunications networks and information systems infrastructure security? What role will government and the private sector play in homeland defense against cyberattacks on critical civilian infrastructure, financial, and logistical systems? What legal impediments exist concerning efforts to defend the nation against cyberattacks, especially in preventive, preemptive, and retaliatory actions? The book is the result of a two-day colloquium titled Cyber Security Infrastructure Protection, conducted in June 2011 by the Center of Information Networking and Telecommunications (CINT) at the Grove School of Engineering, the Colin Powell Center for Public Policy (both at the City University of New York, City College [CCNY]) and the Strategic Studies Institute at the U.S. Army War College. (279 pages)
Cybersecurity: The Nation's Greatest Threat to Critical Infrastructure	U.S. Army War College	March 2013	The paper provides a background on what constitutes national critical infrastructure and critical infrastructure protection; discusses the immense vulnerabilities, threats, and risks associated in the protection of critical infrastructure; and outlines governance and responsibilities of protecting vulnerable infrastructure. The paper makes recommendations for federal responsibilities and legislation to direct national critical infrastructure efforts to ensure national security, public safety, and economic stability. (38 pages)

Title	Source	Date	Notes
NIPP 2013: Partnering for Critical Infrastructure Security and Resilience	Department of Homeland Security (DHS)	2013	The National Infrastructure Protection Plan (NIPP) 2013 meets the requirements of Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," signed in February 2013. The plan was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and all levels of government and industry. It provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes. (57 pages)
Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use	GAO	December 9, 2011	According to GAO, given the plethora of cybersecurity 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 available guidance could help both federal and private-sector decisionmakers better coordinate their efforts to protect critical cyber-reliant assets. (77 pages)
Continued Attention Needed to Protect Our Nation's Critical Infrastructure	GAO	July 26, 2011	A number of significant challenges remain to enhancing the security of cyber-reliant critical infrastructures, such as (1) implementing actions recommended by the President's cybersecurity policy review; (2) updating the national strategy for securing the information and communications infrastructure; (3) reassessing DHS's planning approach to critical infrastructure protection; (4) strengthening public-private partnerships, particularly for information sharing; (5) enhancing the national capability for cyber warning and analysis; (6) addressing global aspects of cybersecurity and governance; and (7) securing the modernized electricity grid. (20 pages)
Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems	GAO	March 16, 2011	According to GAO, executive branch agencies have made progress instituting several government-wide initiatives aimed at bolstering aspects of federal cybersecurity, such as reducing the number of federal access points to the Internet, establishing security configurations for desktop computers, and enhancing situational awareness of cyber events. Despite these efforts, the federal government continues to face significant challenges in protecting the nation's cyber-reliant critical infrastructure and federal information systems. (17 pages)

Title	Source	Date	Notes
Partnership for Cybersecurity Innovation	White House Office of Science and Technology Policy	December 6, 2010	The Obama Administration released a memorandum of understanding signed by DOC's NIST, DHS's Science and Technology Directorate (DHS/S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement is to speed up the commercialization of cybersecurity research innovations that support the nation's critical infrastructures. (4 pages)
Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed	GAO	July 15, 2010	Private-sector stakeholders reported that they expect their federal partners to provide usable, timely, and actionable cyber threat information and alerts; access to sensitive or classified information; a secure mechanism for sharing information; security clearances; and a single centralized government cybersecurity organization to coordinate government efforts. However, according to private-sector stakeholders, federal partners are not consistently meeting these expectations. (38 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are webpages.

Table 2. Energy Sector

(includes electrical grid, smart grid, SCADA, and industrial control systems)

Title	Source	Date	Notes
Cybersecurity for Energy Delivery Systems Program (CEDS)	Department of Energy (DOE), Office of Electricity Delivery and Energy Reliability	Continuously Updated	The program assists the energy-sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.
Cybersecurity Capability Maturity Model (C2M2)	DOE Office of Electricity Delivery and Energy Reliability	Continuously Updated	The model was developed by the DOE and industry as a cybersecurity control evaluation and improvement management tool for energy sector firms. It tells adherents how to assess and grade adoption of cybersecurity practices.

Title	Source	Date	Notes
Cyber Infrastructure Protection	Homeland Security Digital Library (HSDL)	Continuously Updated	HSDL's collection of featured topics related to homeland security topics. Each featured topic is grouped by audits & investigations, CRS reports, DOD reports, executive branch, exercise reports, hearings, international perspective, research & analysis, these, and websites.
GridEx	North American Electric Reliability Corporation (NERC)	Continuously Updated	The objectives of the NERC Grid Security Exercise (GridEx) series are to use simulated scenarios (with *no* real-world effects) to exercise the current readiness of participating electricity subsector entities to respond to cyber or physical security incidents and provide input for security program improvements to the bulk power system. GridEx is a biennial international grid security exercise that uses best practices and other contributions from DHS, the Federal Emergency Management Agency (FEMA), and NIST.
The Energy Sector H4CK3R Report: Profiling the Hacker Groups that Threaten our Nation's Energy Sector	Institute for Critical Infrastructure Technology (ICIT)	August 2016	The report introduces the most prominent actors and exploits, along with hacker group profiles and choice vectors of attack into the conversation of energy sector resiliency to convert bureaucratic babble into a strategic conversation about true and viable security that takes into consideration the complete picture of energy sector vulnerabilities. (56 pages)
Revised Critical Infrastructure Protection Reliability Standards	FERC	July 29, 2016	FERC directs the North American Electric Reliability Corporation to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk Power System. (17 pages)

Title	Source	Date	Notes
Programmable Logic Computers in Nuclear Power Plant Control Systems	Nuclear Regulatory Commission	June 2016	The NRC is denying a petition for rulemaking (PRM), filed by Mr. Alan Morris (petitioner) on March 14, 2013, as supplemented most recently on December 19, 2013. The petitioner requested that the NRC require that his "new-design programmable logic computers [PLCs]" be installed in the control systems of nuclear power plants to block malware attacks on the industrial control systems of those facilities. In addition, the petitioner requested that nuclear power plant staff be trained "in the programming and handling of the non-rewriteable memories" for nuclear power plants. (4 pages)
Cyber Security at Fuel Cycle Facilities	Nuclear Regulatory Commission	April 12, 2016	The NRC is making available a final regulatory basis document to support a rulemaking that would amend its regulations by adopting new cyber security requirements for certain nuclear fuel cycle facility (FCF) licensees to address safety, security, and safeguards. The NRC is not seeking public comments on this document. There will be an opportunity for formal public comment on the proposed rule when it is published in the *Federal Register*. The NRC is making documents publicly available on the federal rulemaking website, www.regulations.gov, under Docket ID NRC–2015–0179. (1 page)
Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System - National Security Perspective	Johns Hopkins University Applied Physics Laboratory	April 2016	The study summarizes restoration challenges posed by Superstorm Sandy and contrasts them with those that would be produced by a cyberattack on the grid. The study then examines the implications of these disparate challenges for the electricity industry's mutual assistance system and proposes potential steps to build an "all-hazards" system that can account for the unique problems that cyberattacks will create. The study also analyzes support missions that state and federal agencies might perform in response to requests for assistance from utilities and how to build a cyber response framework that can coordinate such requests. The study concludes by examining how utilities might prepare in advance for post-cyberattack opportunities to strengthen the architecture of the grid in ways that are not politically or economically feasible today. (66 pages)

Title	Source	Date	Notes
FBI Cyber Bulletin: Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector	FBI	March 31, 2016	The FBI and the US Department of Agriculture (USDA) assess the Food and Agriculture (FA) Sector is increasingly vulnerable to cyberattacks as farmers become more reliant on digitized data. Although precision agriculture technology (a.k.a. smart farming) reduces farming costs and increases crop yields, farmers need to be aware of and understand the associated cyber risks to their data and ensure that companies entrusted to manage their data, including digital management tool and application developers and cloud service providers, develop adequate cybersecurity and breach response plans. (6 pages)
Revised Critical Infrastructure Protection (CIP) Reliability Standards	Federal Energy Regulatory Commission (FERC)	January 26, 2016	The proposed reliability standards address the cybersecurity of the bulk electric system and improve upon the current commission-approved CIP Reliability Standards. In addition, the commission directs NERC to develop certain modifications to improve the CIP Reliability Standards. (15 pages)
Revised Critical Infrastructure Protection Reliability Standards; Supplemental Notice of Agenda and Discussion Topics for Staff Technical Conference	FERC	December 28, 2015	In a July 22, 2015, Notice of Proposed Rulemaking (NOPR), FERC proposed to direct the NERC to develop new or modified CIP Reliability Standards to provide security controls relating to supply chain risk management for industrial control system hardware, software, and services. The commission sought and received comments on this proposal. (3 pages)
Transmission Operations Reliability Standards and Interconnection Reliability Operations and Coordination Reliability Standards	FERC	November 27, 2015	FERC approves revisions to the standards developed by NERC, which the commission has certified as the Electric Reliability Organization responsible for developing and enforcing mandatory reliability standards. The commission also directs NERC to make three modifications to the standards within 18 months of the effective date of the final rule. (15 pages)
Cyber Security Event Notifications	Nuclear Regulatory Commission (NRC)	November 2, 2015	This rule establishes new cybersecurity event notification requirements for nuclear power reactor licensees that contribute to the NRC's analysis of the reliability and effectiveness of licensees' cybersecurity programs and plays an important role in the continuing effort to provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design basis threat. (14 pages)

Title	Source	Date	Notes
Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention	GAO	October 21, 2015	In a 2011 report, GAO recommended that (1) NIST improve its cybersecurity standards, (2) FERC assess whether challenges identified by GAO should be addressed in ongoing cybersecurity efforts, and (3) FERC coordinate with other regulators to identify strategies for monitoring compliance with voluntary standards. The agencies agreed with the recommendations, but FERC has not taken steps to monitor compliance with voluntary standards. (18 pages)
Energy Department Invests Over $34 Million to Improve Protection of the Nation's Energy Infrastructure	DOE	October 9, 2015	DOE announced more than $34 million for two projects to improve the protection of the U.S. electric grid and oil and natural gas infrastructure from cyber threats. The University of Arkansas and the University of Illinois will assemble teams with expertise in power systems engineering and the computer science of cybersecurity to develop new technologies to help protect energy delivery systems that control the physical processes in delivering continuous and reliable power.
Cyber Security at Civil Nuclear Facilities: Understanding the Risk	Chatham House	October 2015	The risk of a serious cyberattack on civil nuclear infrastructure is growing, as facilities become ever more reliant on digital systems and make increasing use of commercial off-the-shelf software. The trend to digitization, when combined with a lack of executive-level awareness of the risks involved, means that nuclear plant personnel may not realize the full extent of their cyber vulnerability and are thus inadequately prepared to deal with potential attacks. (53 pages)
Identity and Access Management for Electric Utilities [DRAFT]	National Institute of Standards and Technology (NIST)	August 24, 2015	To help the energy sector address the cybersecurity challenge, security engineers at the National Cybersecurity Center of Excellence (NCCoE) developed an example solution that utilities can use to more securely and efficiently manage access to the networked devices and facilities upon which power generation, transmission, and distribution depend.

Title	Source	Date	Notes
FACT SHEET: The 2015 G-7 Summit at Schloss Elmau, Germany	White House	June 8, 2015	Member nations of the Group of Seven (G-7) announced a new cooperative effort to guard the energy sector from hackers, cyber spies, and other online attackers. The seven industrialized democracies will exchange information on methods for identifying cyber threats and vulnerabilities within the energy sector, sharing best practices, and making "investment in cybersecurity capabilities and capacity building." See "Launching New Work on Energy Sector Cybersecurity" on the fact sheet.
Energy Sector Cybersecurity Framework Implementation Guidance: Draft For Public Comment and Comment Submission Form	DOE Office of Electricity Delivery and Energy Reliability	September 12, 2014	Energy companies need not make a choice between the NIST cybersecurity framework and the DOE's Cybersecurity Capability Maturity Model (C2M2). The NIST framework tells organizations to grade themselves on a four-tier scale based on their overall cybersecurity program sophistication. C2M2 tells users to assess cybersecurity control implementation across 10 domains of cybersecurity practices, such as situational awareness, according to their specific "maturity indicator level."
Guidelines for Smart Grid Cybersecurity, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements (3 volumes)	NIST	September 2014	The three-volume report presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart-grid stakeholders—from utilities to energy management services providers to electric vehicles and charging stations manufacturers—can use the report's methods and supporting information as guidance to assess risk and identify and apply appropriate security requirements. The approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify. (668 pages)

Title	Source	Date	Notes
Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid	Center for the Study of the Presidency and Congress	July 2014	Although the electrical grid modernization entails significant security challenges, it provides an opportunity to incorporate security—both in the hardware and software controlling these systems and in the business models, regulatory systems, financial incentives, and insurance structures that govern the generation, transmission, and distribution of electric power. The report seeks to identify the immediate action that can be taken by the White House, Congress, and the private sector to mitigate current threats to the electrical grid. (180 pages)
Implementation Status of the Enhanced Cybersecurity Services Program	DHS Office of Inspector General	July 2014	The National Protection Programs Directorate (NPPD) has made progress in expanding the Enhanced Cybersecurity Services program. As of May 2014, 40 critical infrastructure entities were participating in and 22 companies had signed memorandums of agreement to join the program. Although NPPD has made progress, the Enhanced Cybersecurity Services program has been slow to expand because of limited outreach and resources. In addition, cyber threat information sharing relies on NPPD's manual reviews and analysis, which has led to inconsistent cyber threat indicator quality. (23 pages)
Cybersecurity and Connecticut's Public Utilities	Connecticut Public Utilities Regulatory Authority	April 14, 2014	The document is Connecticut's cybersecurity utilities plan to help strengthen defense against possible future cyber threats. Connecticut is the first state to present a cybersecurity strategy in partnership with the utilities sector and will share it with other states working on similar plans. Among other findings, the report recommends that Connecticut commence self-regulated cyber audits and reports and move toward a third-party audit and assessment system. It also makes recommendations regarding local and regional regulatory roles, emergency drills and training, emergency management officials' coordination, and confidential information handling. (31 pages)
Cybersecurity Procurement Language for Energy Delivery Systems	DOE Energy Sector Control Systems Working Group	April 2014	The guidance suggests procurement strategies and contract language to help U.S. energy companies and technology suppliers build in cybersecurity protections during product design and manufacturing. It was "developed through a public-private working group including federal agencies and private industry leaders." (46 pages)

Title	Source	Date	Notes
Internet of things: the influence of M2M data on the energy industry	GigaOm Research	March 4, 2014	The report examines the drivers of machine-2-machine (M2M)-data exploitation in the smart-grid sector and the oil and gas sector, as well as the risks and opportunities for buyers and suppliers of the related core technologies and services. (21 pages)
Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat	Bipartisan Policy Center	February 28, 2014	The Bipartisan Policy Center's initiative identifies urgent priorities, including strengthening existing protections, enhancing coordination at all levels, and accelerating the development of robust protocols for response and recovery in the event of a successful attack. The initiative developed recommendations in four policy areas: (1) standards and best practices, (2) information sharing, (3) response to a cyberattack, and (4) paying for cybersecurity. The recommendations target Congress, federal government agencies, state public utility commissions (PUCs), and industry.
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (Case Study)	Carnegie Mellon University Software Engineering Institute	January 23, 2014	ES-C2M2 is a White House initiative, led by DOE in partnership with DHS and representatives of electricity subsector asset owners and operators, to manage dynamic threats to the electric grid. Its objectives are to strengthen cybersecurity capabilities, enable consistent evaluation and benchmarking of cybersecurity capabilities, and share knowledge and best practices. (39 pages)
The Department of Energy's July 2013 Cyber Security Breach	DOE Inspector General	December 2013	According to DOE's inspector general, nearly eight times as many current and former Energy Department staff were affected by a July computer hack than was previously estimated. In August, DOE estimated that the hack affected roughly 14,000 current and former staff, leaking personally identifiable information, such as Social Security numbers, birthdays, and banking information. But the breach apparently affected more than 104,000 people. (28 pages)
Electric Grid Vulnerability: Industry Responses Reveal Security Gaps	Representative Edward Markey and Representative Henry Waxman	May 21, 2013	The report found that less than one-quarter of investor-owned utilities and less than one-half of municipally and cooperatively owned utilities followed through with voluntary standards issued by the Federal Energy Regulatory Commission after the Stuxnet worm struck in 2010. (35 pages)

Title	Source	Date	Notes
Version 5 Critical Infrastructure Protection Reliability Standards (Notice of Proposed Rulemaking)	FERC	April 24, 2013	FERC proposes to approve NERC's Version 5 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-5 through CIP-011-1. The proposed reliability standards, which pertain to the cybersecurity of the bulk electric system, are an improvement over the current commission-approved CIP Reliability Standards because they adopt new cybersecurity controls and extend the scope of the systems that are protected by the existing standards. (18 pages)
Terrorism and the Electric Power Delivery System	National Academies of Science (NAS)	November 2012	Focuses on measures that could make the electric power delivery system less vulnerable to attacks, restore power faster after an attack, and make critical services less vulnerable when delivery of conventional electric power has been disrupted. (146 pages)
Canvassing the Targeting of Energy Infrastructure: The Energy Infrastructure Attack Database	*Journal of Energy Security*	August 7, 2012	The Energy Infrastructure Attack Database (EIAD) is a noncommercial dataset that structures information on reported (criminal and political) attacks to the energy infrastructure worldwide by nonstate actors since 1980.The objective of EIAD was to develop a product that could be broadly accessible and connect to existing available resources. (8 pages)
Smart Grid Cybersecurity: Job Performance Model Report	Pacific Northwest National Laboratory	August 2012	The report outlines the work done to develop a smart-grid cybersecurity certification. The primary purpose was to develop a measurement model that may be used to guide curriculum, assessments, and other development of technical and operational smart-Grid cybersecurity knowledge, skills, and abilities. (178 pages)
Smart-Grid Security	Center for Infrastructure Protection and Homeland Security, George Mason School of Law	August 2012	Highlights the significance of and the challenges with securing the smart grid. (26 pages)
Cybersecurity: Challenges in Securing the Electricity Grid	GAO	July 17, 2012	In a prior report, GAO made recommendations related to electricity grid modernization efforts, including developing an approach to monitor compliance with voluntary standards. These recommendations have not yet been implemented. (25 pages)

Title	Source	Date	Notes
Energy Department Develops Tool with Industry to Help Utilities Strengthen Their Cybersecurity Capabilities	DOE	June 28, 2012	The Cybersecurity Self-Evaluation Tool uses best practices developed for the Electricity Subsector Cybersecurity Capability Maturity Model Initiative, which involved a series of workshops with the private sector to draft a maturity model that can be used throughout the electric sector to better protect the grid.
Cybersecurity Risk Management Process (Electricity Subsector)	DOE Office of Electricity Delivery and Energy Reliability	May 2012	The guideline describes a risk-management process targeted to the specific needs of electricity-sector organizations. Its objective was to build upon existing guidance and requirements to develop a flexible risk-management process tuned to the diverse missions, equipment, and business needs of the electric power industry. (96 pages)
Cybersecurity: Challenges to Securing the Modernized Electricity Grid	GAO	February 28, 2012	As GAO reported in January 2011, securing smart grid systems and networks present a number of key challenges that require attention by government and industry. GAO made several recommendations to the Federal Energy Regulatory Commission aimed at addressing these challenges. The commission agreed with these recommendations and described steps it is taking to implement them. (19 pages)
ICT Applications for the Smart Grid: Opportunities and Policy Implications	Organization for Economic Co-operation and Development (OECD)	January 10, 2012	The report discusses "smart" applications of information and communication technologies (ICTs) for more sustainable energy production, management, and consumption. It outlines policy implications for government ministries dealing with telecommunications regulation, ICT sector and innovation promotion, and consumer and competition issues. (44 pages)
The Future of the Electric Grid	Massachusetts Institute of Technology (MIT)	December 5, 2011	Chapter 1 provides an overview of the status of the electric grid, the challenges and opportunities it faces, and major recommendations. To facilitate selective reading, detailed descriptions of the contents of each section in Chapters 2-9 are provided in each chapter's introduction, and recommendations are collected and briefly discussed in each chapter's final section. (See Chapter 9, "Data Communications, Cybersecurity, and Information Privacy," pages 208-234). (39 pages)

Title	Source	Date	Notes
Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed	GAO	January 12, 2011	GAO recommended that "to reduce the risk that NIST's smart grid cybersecurity guidelines will not be as effective as intended, the Secretary of Commerce should direct the Director of NIST to finalize the agency's plan for updating and maintaining the cybersecurity guidelines, including ensuring it incorporates (1) missing key elements identified in this report, and (2) specific milestones for when efforts are to be completed. Also, as a part of finalizing the plan, the Secretary of Commerce should direct the Director of NIST to assess whether any cybersecurity challenges identified in this report should be addressed in the guidelines." (50 pages)
NIST Finalizes Initial Set of Smart Grid Cyber Security Guidelines	NIST	September 2, 2010	NIST released a three-volume set of recommendations relevant to securing the smart grid. The guidelines address a variety of topics, including high-level security requirements, a risk assessment framework, an evaluation of residential privacy issues, and recommendations for protecting the evolving grid from attacks, malicious code, cascading errors, and other threats.
NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses	DOE, Idaho National Laboratory	May 2010	The report by the National Supervisory Control and Data Acquisition Systems (SCADA) Test Bed (NSTB) program notes that computer networks controlling the electric grid are plagued with security holes that could allow intruders to redirect power delivery and steal data. Many of the security vulnerabilities are strikingly basic and fixable problems. (123 pages)
21 Steps to Improve Cyber Security of SCADA Networks	DOE, Infrastructure Security and Energy Restoration	January 1, 2007	The President's Critical Infrastructure Protection Board and DOE have developed steps to help any organization improve the security of its SCADA networks. The steps are divided into two categories: (1) specific actions to improve implementation and (2) actions to establish essential underlying management processes and policies. (10 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are webpages.

Table 3. Financial Industry Sector

(includes banks, insurance, SEC guidance, FFIEC, FDIC, FSOC, IRS)

Title	Source	Date	Notes
Appendix J: Strengthening the Resilience of Outsourced Technology Services	Federal Financial Institutions Examination Council (FFIEC)	Continuously Updated	The increasing sophistication and volume of cyber threats and their ability to disrupt operations or corrupt data can affect the business resilience of financial institutions and technology service providers (TSPs). Financial institutions and their TSPs need to incorporate the potential impact of a cyber event into their business continuity planning (BCP) process and ensure appropriate resilience capabilities are in place. The changing cyber threat landscape may include risks that must be managed to achieve resilience.
ICBA Data Breach Toolkit	Independent Community Bankers of America (ICBA)	Continuously Updated	ICBA and Visa have teamed up to bring a special communications toolkit to community banks. The comprehensive communications guide gives community banks the means to communicate with card customers and the media within 24 hours of a data compromise. The toolkit includes a brochure on communications best practices following a data breach and customizable template materials, such as cardholder letters, statement inserts, FAQs, and media statements.
Financial Services Information Sharing & Analysis Center (FS-ISAC)	FS-ISAC	Continuously Updated	The Financial Services Information Sharing and Analysis Center, FS-ISAC, is the global financial industry's go to resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members and operates as a member-owned nonprofit entity.
PureFunds ISE Cyber Security ETF	PureFunds	Continuously Updated	The Exchange Traded Fund (ETF) will invest in companies that develop products or provide services tied to malware protection. As concerns over cyberattacks grow, the industry for protecting against unauthorized breaches will expand. The fund seeks to provide investment results that, before fees and expenses, correspond generally to the price and yield performance of the ISE Cyber Security Index.

Title	Source	Date	Notes
Creating a Federally Sponsored Cyber Insurance Program	Council on Foreign Relations	November 2016	The report recommends that a federally sponsored cyber insurance program should use the promise of limited financial liability to promote participation in initiatives that benefit Interne security as a whole and reduce systemic risk. Initially, the government's goal should be to use the program to promote data sharing of incidents so that insurers can accurately price risk and set premiums. Doing so could provide the data necessary to judge the effectiveness of existing best practices and identify new practices that should be widely adopted. (6 pages)
Enhanced Cyber Risk Management Standards	Federal Reserve, Comptroller of the Currency, FDIC	October 26, 2016	The agencies are considering applying the enhanced standards to depository institutions and depository institution holding companies with total consolidated assets of $50 billion or more, the U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more, and financial market infrastructure companies and nonbank financial companies supervised by the Federal Reserve Board. The proposed enhanced standards would not apply to community banks. (12 pages)
System Safeguards Testing Requirements	Commodity Futures Trading Commission (CFTC)	September 19, 2016	The CFTC is adopting final rules amending its current system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories, by enhancing and clarifying current provisions relating to system safeguards risk analysis and oversight and cybersecurity testing, and adding new provisions concerning certain aspects of cybersecurity testing. (49 pages)
System Safeguards Testing Requirements for Derivatives Clearing Organizations	CFTC	September 19, 2016	The CFTC Is adopting enhanced requirements for testing by a derivatives clearing organization (DCO) of its system safeguards, as well as additional amendments to reorder and renumber certain paragraphs within the regulations and make other minor changes to improve the clarity of the rule text. (20 pages)
Science, Space, and Technology Committee's Investigation of FDIC's Cybersecurity	House Science, Space, and Technology Committee (Staff Report)	July 12, 2016	According to congressional investigators, the Chinese government hacked into 12 computers and 10 backroom servers at the FDIC, including the personal computers of the agency's top officials: the FDIC chairman, his chief of staff, and the general counsel. When congressional investigators tried to review the FDIC's cybersecurity policy, the agency hid the hack, according to the report. (25 pages)

Title	Source	Date	Notes
Adviser Business Continuity and Transition Plans (Proposed Rule)	Securities and Exchange Commission (SEC)	July 5, 2016	The proposed rule would require SEC-registered investment advisers to adopt and implement written business continuity and transition plans reasonably designed to address operational and other risks related to a significant disruption in the investment adviser's operations. The proposal would also amend rule 204-2 under the Advisers Act to require SEC-registered investment advisers to make and keep all business continuity and transition plans that are currently in effect or at any time within the past five years were in effect. (27 pages)
FDIC Implemented Controls over Financial Systems, but Further Improvements are Needed	GAO	June 29, 2016	GAO assessed the effectiveness of the FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. To do so, GAO examined security policies, procedures, reports, and other documents; tested controls over key financial applications; and interviewed FDIC personnel. (29 pages)
Guidance on Cyber Resilience for Financial Market Infrastructures	Bank for International Settlements and OICU-IOSCO	June 2016	The Cyber Guidance requires FMIs to instill a culture of cyber risk awareness and to demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organization. The Cyber Guidance does not establish additional standards for FMIs beyond those already set out in the Principles for Financial Market Infrastructures (PFMI). Instead, the document is intended to be supplemental to the PFMI, primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17), and FMI links (Principle 20). (32 pages)
Cyber-Related Sanctions Regulations	Treasury Department Office of Foreign Assets Control (OFAC)	December 31, 2015	OFAC is issuing regulations to implement Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015. OFAC intends to supplement part 578 with a more comprehensive set of regulations, which may include additional interpretive and definitional guidance and additional general licenses and statements of licensing policy. (8 pages)

Title	Source	Date	Notes
Transfer Agent Regulations	SEC	December 31, 2015	See Part E. Cybersecurity, Information Technology, and Related Issues. "Cybersecurity risks faced by the capital markets and Commission-regulated entities are of particular concern to the Commission. Given the highly-dependent, interconnected nature of the U.S. capital markets and financial infrastructure, including the National C&S System, as well as the prevalence of electronic book-entry securities holdings in that system, the Commission has a significant interest in addressing the substantial risks of market disruptions and investor harm posed by cybersecurity issues. Transfer agents are subject to many of the same risks of data system breach or failure that other market participants face." (58 pages)
System Safeguards Testing Requirements	Commodity Futures Trading Commission (CFTC)	December 23, 2015	The CFTC is amending its system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories by (1) enhancing and clarifying existing provisions related to system safeguards risk analysis, oversight, and cybersecurity testing and (2) adding new provisions concerning certain aspects of cybersecurity testing. (53 pages)
FFIEC Releases Statement on Cyber Attacks Involving Extortion	FFIEC	November 3, 2015	FFIEC released a statement describing steps financial institutions can take to respond to cyberattacks involving extortion. The statement highlights resources institutions can use to mitigate the risks posed by such attacks. (3 pages)
Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information	GAO	July 2, 2015	The report's objectives include examining (1) how regulators oversee institutions' efforts to mitigate cyber threats, and (2) sources of and efforts by agencies to share cyber threat information. GAO collected and analyzed cyber security studies from private-sector sources and reviewed materials from selected IT examinations (based on regulator, institution size, and risk level). GAO also held three forums with more than 50 members of financial institution industry associations who provided opinions on cyber threat information sharing. GAO recommended that Congress consider granting NCUA authority to examine third-party technology service providers for credit unions and regulators explore ways to better collect and analyze data on trends in IT examination findings across institutions. (73 pages)

Title	Source	Date	Notes
2015 Annual Report	Financial Stability Oversight Council (FSOC)	April 25, 2015	Under the Dodd-Frank Act, FSOC must report annually to Congress on a range of issues, including significant financial market and regulatory developments and potential emerging threats to the financial stability of the United States. FSOC's recommendations address heightened risk management and supervisory attention to operational risks, including cybersecurity and infrastructure. (150 pages)
National Cybersecurity Center of Excellence Access Rights Management Use Case for the Financial Services Sector	NIST	April 3, 2015	NIST is canvassing for technologies the financial-services sector could use to unify disparate computer logon systems. As part of the agency's National Cybersecurity Center of Excellence ongoing work, the goal is for the center to review technologies that can create a unified "comprehensive identity and access management system" that will streamline the task of multiple applications and automatically monitor activity. (3 pages)
Cybersecurity Guidance	SEC	April 2015	The SEC's Division of Investment Management guidance states that an investment fund that cannot repay shareholders because of a cyberattack risks violating federal securities laws. The guidance recommends that advisors and funds conduct periodic assessments, have a cybersecurity strategy, and have written policies and procedures to mitigate cyberattacks. (6 pages)
Cybersecurity Examination Sweep Summary	SEC	February 3, 2015	The SEC published findings from an assessment of more than 100 broker-dealers and investment advisers initiated in April 2014. More than 90% of broker firms and 80% of advisers had written information security policies, with most of brokerages and just over half of advisers conducting audits. But less than one-third of brokerages and one-fifth of advisers include written policies about responsibilities for client loss in the event of a cyber incident. In addition, although 84% of broker-dealers applied risk assessments to their vendors, only 32% of advisers did. (7 pages)
Annual Assessment of the Internal Revenue Service's Information Technology Program	Department of Treasury Inspector General for Tax Administration	September 30, 2014	The report identifies a list of security weaknesses in the Internal Revenue Service's (IRS's) systems that support the Affordable Care Act. The security control weaknesses could affect the IRS's ability to reliably process insurers' and drug companies' reports electronically. (45 pages)

Title	Source	Date	Notes
OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations	Treasury	September 11, 2014	Interagency guidelines establishing information security standards for national banks, federal branches and agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). (33 pages)
Third-Party Security Assurance Information Supplement	Payment Card Industry (PCI) Security Standards Council	August 7, 2014	The PCI Security Standards Council has created guidelines meant to help banks and merchants mitigate the risks posed by third parties that process credit card payment information. The guidance includes practical recommendations on how to conduct due diligence and risk assessment when engaging third-party service providers to help organizations understand the services provided.
OCIE Cybersecurity Initiative	SEC	April 15, 2014	The SEC's Office of Compliance Inspections and Examinations (OCIE) will be conducting examinations of more than 50 registered broker-dealers and registered investment advisers, focusing on the entity's cybersecurity governance; identification and assessment of cybersecurity risks; protection of networks and information; risks associated with remote customer access and funds transfer requests; risks associated with vendors and other third parties; detection of unauthorized activity; and experiences with certain cybersecurity threats. (9 pages)
Self-Regulatory Organizations; Chicago Board Options Exchange, Incorporated; Notice of Withdrawal of Proposed Rule Change Relating to Multi-Class Spread Orders	SEC	February 24, 2014	The SEC solicited comments on proposed amendments to the Financial Industry Regulatory Authority's (FINRA's) arbitration codes to ensure that parties' private information, such as Social Security and financial account numbers, are redacted to include only the last four digits of the number. The proposed amendments would apply only to documents filed with FINRA. They would not apply to documents that parties exchange with each other or submit to the arbitrators at a hearing on the merits. (1 page)
Cybersecurity Exercise: Quantum Dawn 2	Securities Industry and Financial Markets Association (SIFMA)	October 21, 2013	Quantum Dawn 2 is a cybersecurity exercise to test incident response, resolution, and coordination processes for the financial services sector and the individual member firms to a street-wide cyberattack.
FFIEC Forms Cybersecurity and Critical Infrastructure Working Group	FFIEC	June 6, 2013	FFIEC formed a working group to further promote coordination across federal and state banking regulatory agencies on critical infrastructure and cybersecurity issues. (2 pages)

Title	Source	Date	Notes
Identity Theft Red Flags Rules	CFTC	April 19, 2013	The joint final rule and guidelines require financial institutions and creditors to develop and implement a written identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with certain existing accounts or the opening of new accounts. The rules include guidelines to assist entities in the formulation and maintenance of programs that would satisfy the requirements of the rules. (30 pages)
Regulation Systems Compliance and Integrity	SEC	March 25, 2013	The SEC examined the exposure of stock exchanges, brokerages, and other Wall Street firms to cyberattacks. The proposed rule asked whether stock exchanges should be required to inform members about breaches of critical systems. More than half of exchanges surveyed globally in 2012 said they had experienced a cyberattack, and 67% of U.S. exchanges said hackers tried to penetrate their systems. (104 pages)
Cybersecurity: CF Disclosure Guidance: Topic No. 2	SEC	October 13, 2011	The guidance presents the views of the Division of Corporation Finance regarding "disclosure obligations relating to cybersecurity risks and cyber incidents." It is not a rule, regulation, or statement of the SEC, and the commission has neither approved nor disapproved its content.
Partnership for Cybersecurity Innovation	White House Office of Science and Technology Policy	December 6, 2010	The Obama Administration released a memorandum of understanding signed by DOC's NIST, DHS's Science and Technology Directorate (DHS/S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement was to speed up the commercialization of cybersecurity research innovations that support the nation's critical infrastructures. (4 pages)

Source: Highlights compiled by CRS from the reports

Note: Page counts are documents; other cited resources are webpages.

Table 4. Health Sector

(includes Healthcare.gov, health insurance, Medicaid, medical devices)

Title	Source	Date	Notes
HHS Breach Portal: Breaches Affecting 500 or More Individuals	Health and Human Services (HHS)	Continuously Updated	As required by Section 13402(e)(4) of the HITECH Act (P.L. 111-5), the HHS Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, the new format includes brief summaries of breach cases that optical character recognition (OCR) has investigated and closed, as well as the names of private practice providers that have reported breaches of unsecured protected health information to the Secretary.
Precision Medicine Initiative: Data Security Policy Principles and Framework	White House	May 25, 2016	Personalized treatment for patients is the end-goal of the White House's Precision Medicine Initiative, a $215 million program launched last year. But that data, which might include details about insurance claims, demographics, genomic and biological characteristics, and information transmitted from smartphones or implantable devices, needs to be highly secured. (10 pages)
NCCoE Wireless Medical Infusion Pumps Use Case for the Health Care Sector	National Institute of Standards and Technology (NIST)	January 25, 2016	NIST invites organizations to provide products and technical expertise to support and demonstrate security platforms for the Wireless Medical Infusion Pumps use case for the health care sector. The notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the Health Care Sector program. (3 pages)

Title	Source	Date	Notes
Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff	Food and Drug Administration (FDA)	January 22, 2016	The guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. For the majority of cases, actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered "cybersecurity routine updates or patches," for which the FDA does not require advance notification or reporting under 21 C.F.R. 806. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the Agency. (25 pages)
2015 Protected Health Information Data Breach Report (PHIDBR)	Verizon	December 15, 2015	The study shed light on the problem of medical data loss—how it is disclosed, who is causing it, and what can be done to combat it. Reportedly, 90% of industries have experienced a PHI breach. Since 2009, half of the U.S. population has been affected by PHI breaches. (34 pages)
Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data	Ponemon Institute	May 2015	Reportedly a rise in cyberattacks against doctors and hospitals is costing the U.S. health care system $6 billion a year as organized criminals who once targeted retailers and financial firms increasingly go after medical records. Criminal attacks are up 125% compared with replacing lost laptops as the leading threat five years ago. The study also found most organizations are unprepared to address new threats and lack adequate resources to protect patient data. (7 pages)
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	FDA	October 1, 2014	The guidance, first issued as a draft in June 2013, instructs manufactures to "develop a set of cybersecurity controls." It also instructs manufactures to consider following the core functions of the NIST cybersecurity framework, a model for cybersecurity activities: identify, protect, detect, respond, and recover. (9 pages)

Title	Source	Date	Notes
Collaborative Approaches for Medical Device and Healthcare Cybersecurity; Public Workshop; Request for Comments	FDA	September 23, 2014	In October 2014, the FDA held a public workshop on collaborative approaches for medical device and health care cybersecurity. The FDA, in collaboration with other stakeholders within the HHS and DHS, seeks broad input from the Healthcare and Public Health (HPH) sector on medical device and health care cybersecurity. The workshop's vision was to catalyze collaboration among all HPH stakeholders. (3 pages)
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Notice	(FDA	June 14, 2013	The guidance identifies cybersecurity issues that manufacturers should consider in preparing premarket submissions for medical devices to maintain information confidentiality, integrity, and availability. (1 page)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are webpages.

Table 5. Telecommunications and Communications Sector

(includes wired, wireless, Internet service providers, GPS, undersea cables, public safety broadband network)

Title	Source	Date	Notes
The Communications Security, Reliability and Interoperability Council (CSRIC)	Federal Communications Commission (FCC)	Continuously Updated	The CSRIC mission is to provide recommendations to the FCC to ensure optimal security and reliability of communications systems, including telecommunications, media, and public safety.
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	FCC	December 2, 2016	The FCC adopts this final rules based on public comments applying the privacy requirements of the Communications Act of 1934, as amended, to broadband Internet access service (BIAS) and other telecommunications services. In adopting these rules, the commission implements the statutory requirement that telecommunications carriers protect the confidentiality of customer proprietary information. The privacy framework in these rules focuses on transparency, choice, and data security, and provides heightened protection for sensitive customer information, consistent with customer expectations. (73 pages)

Title	Source	Date	Notes
9-1-1 DDoS: Threat, Analysis and Mitigation	Ben Gurion University of the Negrev	September 8, 2016	Researchers explore the 911 infrastructure and discuss why it is susceptible to this kind of attack. They then implement different forms of the attack and test our implementation on a small cellular network. They simulate and analyze anonymous attacks on a current 911 infrastructure model of to measure the severity of their impact. (15 pages)
Space, the Final Frontier for Cybersecurity?	Chatham House, Royal Institute of International Affairs	September 2016	Analyzing the intersection between cyber and space security is essential to understanding this non-traditional, evolving security threat. Cybersecurity and space security are inextricably linked. Technologies in satellites and other space assets are sourced from a broad international supply base and therefore require regular security upgrades. And the upgrades via remote connections could serve to make space assets vulnerable to cyberattacks. In everyday life, satellites are regularly used to provide Internet services and global navigation satellite system (GNSS) technologies that are increasingly embedded in almost all critical infrastructures. (46 pages)
Disruptions to Communications	FCC	July 12, 2016	The FCC seeks comment on a proposal to update the commission's outage reporting requirement rules to address broadband network disruptions, including packet- based disruptions based on network performance degradation; proposed changes to the rules governing interconnected voice over Internet protocol (VoIP) outage reporting to include disruptions based on network performance degradation, update the outage definition to address incidents involving specified network components; and modify the reporting process to make it consistent with other services; reporting of call failures in the radio access network and local access network, and on geography-based reporting of wireless outages in rural areas; and, refining the covered critical communications at airports subject to the commission's outage reporting requirements. (24 pages)
FirstNet's Nationwide Public Safety Broadband Network (NPSBN)	FirstNet (National Telecommunications and Information Administration, NTIA)	October 5, 2015	FirstNet is requesting feedback from stakeholders, including states, tribes, territories, public safety stakeholders, and market participants, on Appendix C-10 NPSBN Cyber Security that will inform the development of the cybersecurity portions of the nationwide public safety broadband network (NPSBN). (3 pages)

Title	Source	Date	Notes
Cybersecurity Risk Management and Best Practices (WG4): Cybersecurity Framework for the Communications Sector	FCC, CSRIC	March 18, 2015	The CSRIC is a federal advisory committee that provides recommendations to the FCC regarding best practices and actions the commission can take to help ensure security, reliability, and interoperability of communications systems and infrastructure. The CSRIC approved a report that identifies best practices, provides a variety of important tools and resources for communications companies of different sizes and types to manage cybersecurity risks, and recommends a path forward. (415 pages)
Security in the New Mobile Ecosystem	Ponemon Institute and Raytheon	August 2014	Mobile devices are quickly becoming an integral tool for the workforce, but the security practices and budgets in most organizations are not keeping pace with the growing number of devices that must be managed and kept secure. (Free registration required.) (30 pages)
Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators	Carnegie Mellon/Pittsburgh Software Institute	March 2014	The WEA service depends on computer systems and networks to convey potentially life-saving information to the public in a timely manner. However, like other cyber-enabled services, it is susceptible to risks that may enable attackers to disseminate unauthorized alerts or to delay, modify, or destroy valid alerts. Successful attacks may result in property destruction, financial loss, injury, or death and may damage WEA credibility to the extent that users ignore future alerts or disable alerting. The report describes a four-stage cybersecurity risk management (CSRM) strategy that alert originators can use throughout WEA adoption, operations, and sustainment, as well as a set of governance activities for developing a plan to execute the CSRM. (183 pages)
Mobile Security Reference Architecture	Federal CIO Council and DHS	May 23, 2013	The document guides agencies in the secure implementation of mobile solutions through their enterprise architectures. It provides in-depth reference architecture for mobile computing. (103 pages)

Title	Source	Date	Notes
Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment	GAO	May 21, 2013	The federal government began efforts to address the security of commercial networks' supply chain. A variety of approaches to address the potential risks posed by foreign-manufactured equipment in commercial communications networks include those taken by foreign governments. Although these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers, additional costs, and constraints on competition, which the federal government would have to take into account if it chose to pursue such approaches. (52 pages)
Comments on Incentives to Adopt Improved Cybersecurity Practices	National Institute Of Standards And Technology (NIST) and the National Telecommunications and Information Administration	April 29, 2013	DOC investigated ways to incentivize companies and organizations to improve their cybersecurity. To better understand what stakeholders—such as companies, trade associations, academics, and others—believe would best serve as incentives, the department released public comments to the notice of inquiry.
Open Trusted Technology Provider Standard (O-TTPS)™, Version 1.0: Mitigating Maliciously Tainted and Counterfeit Products	The Open Group	April 2013	Specifically intended to prevent maliciously tainted and counterfeit products from entering the supply chain, the first release of the O-TTPS codifies best practices across the entire commercial, off-the-shelf information and communication technology product life cycle, including the design, sourcing, building, fulfillment, distribution, sustainment, and disposal phases. The O-TTPS will enable organizations to implement best practice requirements and allow all providers, component suppliers, and integrators to obtain trusted technology provider status. (Registration required.) (44 pages)
Privacy and Security of Information Stored on Mobile Communications Devices	FCC	June 13, 2012	The proposed rule seeks comment on the privacy and data security practices of mobile wireless services providers with respect to customer information stored on their users' mobile communications devices. (3 pages)
FCC's Plan for Ensuring the Security of Telecommunications Networks	FCC	June 3, 2011	FCC Chairman Genachowski's response to a letter from Representative Anna Eshoo dated November 2, 2010, regarding concerns about the implications of foreign-controlled telecommunications infrastructure companies providing equipment to the U.S. market. (1 page)

Title	Source	Date	Notes
Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk	GAO	November 30, 2010	Existing government-wide guidelines and oversight efforts do not fully address agency implementation of leading wireless security practices. Until agencies take steps to better implement these leading practices and OMB takes steps to improve government-wide oversight wireless, networks will remain at an increased vulnerability to attack. (50 pages)
The Reliability of Global Undersea Communications Cable Infrastructure (The ROGUCCI Report)	Institute of Electrical and Electronics Engineers and the EastWest Institute	May 26, 2010	The study submits 12 major recommendations to private-sector, government, and other stakeholders—especially the financial sector—for the purpose of improving the reliability, robustness, resilience, and security of the world's undersea communications cable infrastructure. (186 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are webpages.

Table 6. Transportation

(includes Coast Guard, air traffic control, ports and maritime, automobiles)

Title	Source	Date	Notes
Cybersecurity	Homeport, U.S. Coast Guard	Continuously Updated	Links to regulations, guidelines, advisories & alerts, and news pertaining to maritime cybersecurity.
Letter to Federal Communications Commission re: vehicle-to-vehicle communications	Senators Ed Markey and Richard Blumenthal	August 4, 2016	The Senators said the FCC should ensure that spectrum set aside for the vehicle-to-vehicle transmissions, also known as Dedicated Short Range Communications, is only used for safety applications. (3 pages)
Automotive Cybersecurity Best Practices: Executive Summary	Automotive Information Sharing and Analysis Center	July 21, 2016	The best practices are meant to serve as guidance in the development of automotive cybersecurity in seven key areas: governance, risk assessment and management, security by design, threat detection and protection, incident response, awareness and training, and collaboration and engagement with appropriate third parties. (8 pages)

Title	Source	Date	Notes
Request for Public Comments on NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Emerging Automotive Technologies	National Highway Traffic Safety Administration	April 1, 2016	The proposed Enforcement Guidance Bulletin sets forth NHTSA's current views on emerging automotive technologies—including its view that when vulnerabilities of such technology or equipment pose an unreasonable risk to safety, those vulnerabilities constitute a safety-related defect—and suggests guiding principles and best practices for motor vehicle and equipment manufacturers in this context. (5 pages)
Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack	GAO	March 24, 2016	This report addresses, among other things, (1) available information about the key cybersecurity vulnerabilities in modern vehicles that could impact passenger safety; (2) key practices and technologies, if any, available to mitigate vehicle cybersecurity vulnerabilities and the impacts of potential attacks; (3) views of selected stakeholders on challenges they face related to vehicle cybersecurity and industry-led efforts to address vehicle cybersecurity; and (4) DOT efforts to address vehicle cybersecurity. (61 pages)
Guidelines on Cyber Security Onboard Ships	Baltic and International Maritime Council (BIMCO)	January 4, 2016	A first set of guidelines for the shipping industry contain information on understanding cyber threats, how to assess and reduce risks, how to develop contingency plans, and identifying vulnerabilities and potential targets for cybercriminals. (36 pages)
Section 1201 Rulemaking, Proposed Exemptions of Vehicle Software	Department of Transportation (DOT) General Counsel	September 9, 2015	DOT "is concerned that there may be circumstances in which security researchers may not fully appreciate the potential safety ramifications" if their findings are released to the public, according to a DOT letter to federal Intellectual Property regulators, who are considering a proposal to allow the public to circumvent copyright protection measures attached to vehicle software. (3 pages)
United States Coast Guard Cyber Strategy	U.S. Coast Guard	June 16, 2015	Among the concrete objectives is development of formal guidance for commercial vessel and waterfront facility operators on evaluating cybersecurity vulnerabilities, which the Coast Guard began in January 2015, when it kicked off a public process that will result in issuance of a Navigation and Vessel Inspection Circular. The document details how cybersecurity will become an element of Maritime Transportation Security Act (P.L. 107-295) enforcement. (44 pages)

Title	Source	Date	Notes
Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk	Sen. Edward Markey	February 11, 2015	Nearly all modern vehicles have some sort of wireless connection that could potentially be used by hackers to remotely access their critical systems. Companies' protections on those connections are "inconsistent and haphazard" across the industry. In addition to security weaknesses, the survey also found that many auto companies are collecting detailed location data through pre-installed technological systems in cars and often transmitting it insecurely. (14 pages)
Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors	Senate Armed Services Committee	September 17, 2014	Hackers associated with the Chinese government successfully penetrated the Transportation Command (TRANSCOM) contractors' computer systems 20 times in a single year. Chinese hackers tried to get into the systems 50 times. The congressional committee found that only two of the intrusions were detected. It also found that officials were unaware due in large part to unclear requirements and methods for contractors to report breaches and for government agencies to share information. (52 pages)
WIB Security Standard Released	International Instrument Users Association (WIB)	November 10, 2010	The Netherlands-based WIB, an international organization that represents global manufacturers in the industrial automation industry, announced the second version of the *Process Control Domain Security Requirements for Vendors* document—the first international standard that outlines a set of specific requirements focusing on cybersecurity best practices for industrial automation and control systems suppliers.

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are webpages.

Author Contact Information

Rita Tehan
Information Research Specialist
rtehan@crs.loc.gov, 7-6739