Cybersecurity: Federal Government Authoritative Reports and Resources

October 13, 2016 (R44427)
Jump to Main Text of Report

Contents

- Introduction

Tables

- Table 1. Federal Government: Overview Reports and Resources
- Table 2. Federal Acquisitions Rules and Federal Contractors
- Table 3. Agency Audits and Evaluations
- Table 4. Federal Workforce
- Table 5. White House and Office of Management and Budget
- Table 6. Cybersecurity Framework (NIST) and Information Sharing
- Table 7. Department of Homeland Security (DHS)
- Table 8. Department of Defense (DOD)
- Table 9. National Institute of Standards and Technology (NIST)

Summary

This report serves as a starting point for congressional staff assigned to cover cybersecurity issues related to federal and military government activities. Much is written by and about the federal government's efforts to address cybersecurity policy challenges, 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. 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

- **Table 1**, overview reports;
- **Table 2**, federal acquisitions rules and federal contractors;
- **Table 3**, federal agency audits and evaluations, including Government Accountability Office (GAO);
- **Table 4**, federal workforce;
- **Table 5**, White House and Office of Management and Budget (OMB);
- **Table 6**, cybersecurity framework and information sharing;
- **Table 7**, Department of Homeland Security (DHS);
- **Table 8**, Department of Defense (DOD); and
- **Table 9**, National Institute of Standards and Technology (NIST).

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

- CRS Report R44405, *Cybersecurity: Overview Reports and Links to Government, News, and Related Resources*, by [author name scrubbed]
- CRS Report R44406, *Cybersecurity: Education, Training, and R&D Authoritative Reports and Resources*, by [author name scrubbed]
- CRS Report R44408, *Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources*, by [author name scrubbed]
- CRS Report R44410, *Cybersecurity: Critical Infrastructure Authoritative Reports and Resources*, by [author name scrubbed]
- CRS Report R44417, *Cybersecurity: State, Local, and International Authoritative Reports and Resources*, by [author name scrubbed]
- CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by [author name scrubbed]
- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by [author name scrubbed]

For access to additional CRS reports and other resources, see the *Cybersecurity Issue Page* at http://www.crs.gov.

Cybersecurity: Federal Government Authoritative Reports and Resources

Introduction

This report serves as a starting point for congressional staff assigned to cover cybersecurity issues related to federal and military agency activities. Much is written by and about the federal government's efforts to address cybersecurity policy and practical challenges, 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. 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

- **Table 1**, overview reports;
- **Table 2**, federal acquisitions rules and federal contractors;
- **Table 3**, federal agency audits and evaluations, including Government Accountability Office (GAO);
- **Table 4**, federal Workforce;
- **Table 5**, White House and Office of Management and Budget (OMB);
- **Table 6**, cybersecurity framework and information sharing;
- **Table 7**, Department of Homeland Security (DHS);
- **Table 8**, Department of Defense (DOD); and
- **Table 9**, National Institute of Standards and Technology (NIST).

Table 1. Federal Government: Overview Reports and Resources

Title	Source	Date	Notes
GAO reports on cybersecurity	GAO	Continuously Updated	A list of five "Key Reports," and dozens of other cybersecurity reports by GAO.
National Strategy for Trusted	National Institute of	Continuously	The NSTIC pilot projects seek to catalyze a marketplace of online identity solutions that ensures the envisioned Identity Ecosystem is trustworthy and reliable. Using privacy-enhancing architectures in real-world

Identities in Cyberspace (NSTIC)	Standards and Technology (NIST)	Updated	environments, the pilots are testing new methods for online identification for consumers that increase usability, security, and interoperability to safeguard online transactions.
Federal cybersecurity initiatives timeline - Draft 1.b	Center for Strategic and International Studies (CSIS)	Continuously Updated	A timeline of presidential and congressional cybersecurity initiatives from 1998 to the present.
Cyber-Related Sanctions Regulations	Office of Foreign Assets Control of the U.S. Department of the Treasury (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 this 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)
Comments on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem	National Telecommunications and Information Administration (NTIA)	June 1, 2015	Public comments to the NTIA regarding its new voluntary cybersecurity project three main areas of industry and researcher concern: (1) the Internet of Things, (2) vulnerability disclosure, and (3) malware.
2016 Internet Security Threat Report | Government	Symantec	April 13, 2016	Public-sector data breaches exposed some 28 million identities in 2015, but hackers were responsible for only one-third of those compromises, according to new research. Negligence was behind nearly two-thirds of the exposed identities through government agencies. In total, the report suggests 21 million identities were compromised accidentally, compared with 6 million by hackers.
Formation of the Office of Technology Research and Investigation (OTRI)	Federal Trade Commission (FTC)	March 23, 2015	The OTRI will provide expert research, investigative techniques, and further insights to the agency on technology issues involving all facets of the FTC's consumer protection mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things.
Stakeholder Engagement on Cybersecurity in the Digital Ecosystem	NTIA	March 19, 2015	"The Internet Policy Task Force (IPTF) is requesting comment to identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers. The IPTF invites public comment on these issues from all stakeholders with an interest in cybersecurity, including the commercial, academic, and civil society sectors, and

			from relevant federal, state, local, and tribal entities." (4 pages)
Federal Incident Reporting Guidelines	United States Computer Emergency Readiness Team (US-CERT)	October 1, 2014	The guidance instructs federal agencies to classify incidents according to their impacts rather than by categories of attack methods. It modifies a 2007 requirement for agencies to report to US-CERT within an hour any incident involving the loss of personally identifiable information (PII). Rather, agencies should notify US-CERT of a confirmed cyber incident within one hour of it reaching the attention of an agency's security operations center or IT department. The Office of Management and Budget (OMB) said in a concurrently released memo that nonelectronic losses of PII must also be reported within an hour of a confirmed breach but should be reported to the agency privacy office rather than US-CERT. (10 pages)
Measuring What Matters: Reducing Risks by Rethinking How We Evaluate Cybersecurity	National Academy of Public Administration and Safegov.org	March 2013	Federal agencies and their inspectors general should keep running scorecards of "cyber risk indicators" based on continual information governance assessments of a their organization's cyber vulnerabilities, rather than periodically auditing whether an agency's systems meet the standards enumerated in the Federal Information Security Management Act (FISMA) at a static moment in time. (39 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources ae web pages.

Table 2. Federal Acquisitions Rules and Federal Contractors

(including regulations, guidance documents, and audit reports)

Title	Source	Date	Notes
Cybersecurity Services	General Services Administration (GSA)	April 11, 2016	GSA's Federal Acquisition Service (FAS) Office of Integrated Technology Services (ITS) is conducting business channel research to gain an enhanced understanding of what agencies' needs are, what solutions currently exist, and what role GSA can play in improving the ability of agencies to procure the suite of cybersecurity services. This information will help GSA identify current offerings available, improve the visibility of those offerings, and determine gaps that need to be filled.
Fiscal Year 2015 Top Management Challenges	Office of Personnel Management (OPM), Office of Inspector	October 30, 2015	See Internal Challenges section (pp. 10-19) for a discussion of challenges related to information technology, improper payments, the retirement claims process, and the procurement process. Officials in OPM's Office of Procurement Operations violated the Federal Acquisition Regulation and the agency's own policies in awarding a $20.7 million contract to provide credit monitoring and ID theft services. Investigators turned up "significant deficiencies"

	General (OIG)		in the process of awarding the contract to Winvale Group and its subcontractor CSID. (22 pages)
Improving Cybersecurity Protections in Federal Acquisitions Public Comment Space	Office of Management and Budget (OMB)	August 10, 2015	OMB proposed that agencies make private-sector adherence to cybersecurity controls a contractual requirement. It is also proposed that contractors operating systems on behalf of federal agencies earn an official approval known as an "Authority to Operate," and that vendors implement a program of continuous monitoring. Also, under an existing policy, security controls for the private sector handling of "controlled unclassified information" will become mandatory for civilian agency contractors in 2016.
Request for Comments on Improving Cybersecurity Protections in Federal Acquisitions	OMB	July 30, 2015	OMB's Office of E-Government & Information Technology (E-Gov) is seeking public comment on draft guidance to improve cybersecurity protections in federal acquisitions. The increase in threats facing federal information systems demand that certain issues regarding security of information on these systems is clearly, effectively, and consistently addressed in federal contracts. (1 page)
Information Security: Agencies Need to Improve Oversight of Contractor Controls	Government Accountability Office (GAO)	September 8, 2014	Although the six federal agenciesâ€”the Departments of Energy, Homeland Security, State, and Transportation; the Environmental Protection Agency; and the Office of Personnel Managementâ€”that GAO reviewed generally established security and privacy requirements and planned effectiveness assessments of contractor implementation of controls, five of the six agencies were inconsistent in overseeing the execution and review of those assessments, resulting in security lapses. For example, in one agency, testing did not discover that background checks of contractor employees were not conducted. (43 pages)
Cybersecurity for Government Contractors	Robert Nichols et al., West Briefing Papers	April 2014	The briefing paper presents a summary of the key legal issues and evolving compliance obligations that contractors now face in the federal cybersecurity landscape. It provides an overview of the most prevalent types of cyberattacks and targets and the federal cybersecurity budget; outlines the current federal cybersecurity legal requirements applicable to government contractors, including statutory and regulatory requirements, the President's 2013 cybersecurity executive order, the resulting "cybersecurity framework" issued by NIST in February 2014; highlights further expected developments; and identifies and discusses the real-world legal risks that contractors face when confronting cyberattacks and addresses the availability of possible liability backstops in the face of such attacks. (28 pages)
Improving Cybersecurity and Resilience through Acquisition	Department of Defense (DOD) and the GSA	January 23, 2014	DOD and GSA jointly released a report announcing six planned reforms to improve the cybersecurity and resilience of the Federal Acquisition System. The report provides a path forward to aligning federal cybersecurity risk management and acquisition processes. It provides strategic recommendations for addressing relevant issues, suggests how challenges might be resolved, and identifies important considerations for the implementation of the recommendations. (24 pages)
			The regulation imposed two new requirements: (1) an obligation

Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information	DOD	November 18, 2013	on contractors to provide adequate security to safeguard unclassified controlled technical information (UCTI) and (2) contractors' obligation to report cyber incidents that affect UCTI to contracting officers. In both obligations, UCTI is defined as "technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination." This is the first time DOD has imposed specific requirements for cybersecurity that are generally applicable to all contractors. (10 pages)
Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, Notice of Request for Information	GSA	May 13, 2013	Among other things, Presidential Policy Directive-21requires GSA, in consultation with DOD and the Department of Homeland Security (DHS), to jointly provide and support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure. (3 pages)
Basic Safeguarding of Contractor Information Systems (Proposed Rule)	DOD, GSA, and National Aeronautics and Space Administration (NASA)	August 24, 2012	This regulation, authored by DOD, GSA, and NASA, "would add a contract clause to address requirements for the basic safeguarding of contractor information systems that contain or process information provided by or generated for the government (other than public information)." (4 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are web pages.

Table 3. Agency Audits and Evaluations

(reports evaluating agency cybersecurity programs, excluding DHS and DOD, see Tables 7 and 8 below)

Title	Source	Date	Notes
GAO reports on cybersecurity	GAO	Continuously Updated	A list of five"Key Reports," and dozens of other cybersecurity reports by GAO.
Pulse: How Federal Government Domains are Meeting Best Practices on the Web	General Services Administration (GSA)	Continuously Updated	Pulse.cio.gov is a public dashboard that displays how well all federal domains are performing in accordance with government-wide web policy requirements and best practices. The first release of Pulse covers two areas of federal web policyâ€”Secure Hypertext Transfer Protocol (HTTPS) and the Digital Analytics Program (DAP).
			The FDA did not fully or consistently implement access

FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk	GAO	September 29, 2016	controls, which are intended to prevent, limit, and detect unauthorized access to computing resources. Specifically, FDA did not always (1) adequately protect the boundaries of its network, (2) consistently identify and authenticate system users, (3) limit users' access to only what was required to perform their duties, (4) encrypt sensitive data, (5) consistently audit and monitor system activity, and (6) conduct physical security reviews of its facilities. (59 pages)
Federal Information Security: Actions Needed to Address Challenges	GAO	September 19, 2016	Cyber incidents affecting federal agencies have continued to grow, increasing about 1,300% from FY2006 to FY2015. Several laws and policies establish a framework for the federal government's information security and assign implementation and oversight responsibilities to key federal entities, including the Office of Management and Budget (OMB), executive branch agencies, and the Department of Homeland Security (DHS). However, implementation of this framework has been inconsistent, and additional actions are needed. (17 pages)
HHS Needs to Strengthen Security and Privacy Guidance and Oversight	GAO	August 1, 2016	In 2015, 113 million electronic health records were breached, a major leap over the 12.5 million the year before. In 2009, the number was less than 135,000. The number of reported hacks and breaches affecting records of at least 500 individuals rose from none in 2009 to 56 last year, almost double from 2014.
Work Plan: Status of Audit and Evaluation Projects	Federal Reserve Office of Inspector General	July 8, 2016	The growing sophistication and volume of cybersecurity threats presents a serious risk to all financial institutions. The report reviews how the Federal Reserve System's examination process has evolved and whether it is providing adequate oversight of financial institutions' information security controls and cybersecurity threats. The Fed has already developed guidance for banks "to define expectations for information security and data breach management." Now the watchdog agency will review howâ€”and ifâ€”banks are complying with that guidance. (43 pages; see pp. 4-5)
FDIC Implemented Controls over Financial Systems, but Further Improvements are Needed	GAO	June 29, 2016	As part of its audit of the 2015 financial statements of the Deposit Insurance Fund and the Federal Savings and Loan Insurance Corporation Resolution Fund administered by FDIC, GAO assessed the effectiveness of the corporation'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)
			Federal systems categorized as high impactâ€”those that

Agencies Need to Improve Controls over Selected High-Impact Systems	GAO	June 21, 2016	hold sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harmâ€”warrant increased security to protect them. In this report, GAO (1) describes the extent to which agencies have identified cyber threats and have reported incidents involving high-impact systems, (2) identifies government-wide guidance and efforts to protect these systems, and (3) assesses the effectiveness of controls to protect selected high-impact systems at federal agencies. To do this, GAO surveyed 24 federal agencies; examined federal policies, standards, guidelines and reports; and interviewed agency officials (94 pages)
Management Report: Areas for Improvement in the Federal Reserve Banks' Information Systems Controls	GAO	June 6, 2016	The report presents the deficiencies identified during GAO's FY2015 testing of information systems controls over key financial systems maintained and operated by Federal Reserve Banks on behalf of Treasury that are relevant to the Schedule of Federal Debt. The report also includes the results of GAO's FY2015 follow-up on the status of FRBs' corrective actions to address information systems control-related deficiencies and associated recommendations contained in GAO's prior years' reports that were open as of September 30, 2014. (9 pages)
Federal Agencies Need to Address Aging Legacy Systems	GAO	May 26, 2016	GAO is making 16 recommendations, one of which is for OMB to develop a goal for its spending measure and finalize draft guidance to identify and prioritize legacy IT needing to be modernized or replaced. GAO is also recommending that selected agencies address at-risk and obsolete legacy O&M investments. (87 pages)
Second Interim Status Report on the U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project â€“ Major IT Business Case	OPM	May 18, 2016	The report finds that funding for the troubled IT security upgrades project remains an issue in part because of poor planning by the agency. The inspector general finds that the agency still lacks a "realistic budget" for the massive upgrade. (12 pages)
Polar Weather Satellites: NOAA Is Working to Ensure Continuity but Needs to Quickly Address Information Security Weaknesses and Future Program	GAO	May 17, 2016	Although the National Oceanic and Atmospheric Administration (NOAA) established information security policies in key areas recommended by the National Institute of Standards and Technology, the Joint Polar Satellite System (JPSS) program has not yet fully implemented them. Specifically, the program categorized the JPSS ground system as a high-impact system and selected and implemented multiple relevant security controls. However, the program has not yet fully implemented almost half of the recommended security controls, did not have all of the information it needed

Uncertainties			when assessing security controls, and has not addressed key vulnerabilities in a timely manner. Until NOAA addresses these weaknesses, the JPSS ground system remains at high risk of compromise. (70 pages)
Management Alert Report: GSA Data Breach	General Services Administration Office of Inspector General	May 12, 2016	The inspector general of the General Services Administration said the 18F tech squad should stop using Slack after the group messaging app was linked to an internal data breach. As part of an audit report, the IG found that 18F's configuration of Slack had allowed access to more than 100 Google Drive accounts inside the agency, resulting in a data breach that potentially exposed "sensitive content" like personal information. According to the report, a supervisor said the issue has been fixed, but the IG said 18F "should cease using Slack" until it's approved as a "standard product" under agency rules. (4 pages)
Information Security: Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data	GAO	April 28, 2016	The report details weaknesses GAO identified in the information security program at SEC during its audit of the commission's FY2015 and FY2014 financial statements. GAO's objective was to determine the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of SEC's key financial systems and information. To do this, GAO examined information security policies, plans, and procedures; tested controls over key financial applications; interviewed agency officials; and assessed corrective actions taken to address previously reported weaknesses. (26 pages)
Final Memorandum, Review of NASA's Information Security Program	National Aeronautics and Space Administration	April 14, 2016	Although NASA has made progress in meeting requirements in support of an agency-wide information security program, it has not fully implemented key management controls essential to managing that program. Specifically, NASA lacks an agency-wide risk management framework for information security and information security architecture. (17 pages)
Information Security: IRS Needs to Further Enhance Controls over Taxpayer and Financial Data	GAO	April 14, 2016	The statement discusses (1) IRS's information security controls over tax processing and financial systems and (2) roles that federal agencies with government-wide information security responsibilities play in providing guidance and oversight to agencies. The statement is based on previously published GAO work and a review of federal guidance. (22 pages)
Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to	GAO	March 24, 2016	The 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

Define Its Role in Responding to a Real-world Attack			cybersecurity and industry-led efforts to address vehicle cybersecurity; and (4) DOT efforts to address vehicle cybersecurity. (61 pages)
Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls	GAO	March 23, 2016	GAO was asked to review security issues related to the data hub, and CMS oversight of state-based marketplaces. Its objectives were to (1) describe security and privacy incidents reported for Healthcare.gov and related systems, (2) assess the effectiveness of security controls for the data hub, and (3) assess CMS oversight of state-based marketplaces and the security of selected state-based marketplaces. GAO reviewed incident data, analyzed networks and controls, reviewed policies and procedures, and interviewed CMS and marketplace officials. (55 pages)
Audit of the EPA's compliance with the mandated "Inspector General Report or Personally Identifiable Information	EPA	March 14, 2016	EPA's inspector general's office said it will "determine to what extent the EPA implemented information system security policies and procedures to protect agency systems" under cybersecurity provisions contained in the 2015 omnibus spending package (P.L. 114-113). The IG will examine the Office of Administrative Services Information System, which contains a wealth of employee personal information to facilitate agency administration, and the Superfund Cost Recovery Package Imaging Online System, which is used to detail government and contractor expenses related to Superfund cleanup. (8 pages)
Assessing the FDA's Cybersecurity Guidelines for Medical Device Manufacturers: Why Subtle "Suggestions" May Not Be Enough	Institute for Critical Infrastructure Technology	February 15, 2016	The guidance advises medical device manufacturers to address cybersecurity "throughout a product's lifecycle" and is the latest action by the FDA that underscores its position that medical device cybersecurity is a priority for the health sector. However, despite the implied sense of urgency, the FDA has chosen not to implement enforceable regulations over medical device manufacturers. This examination of the FDA's 'suggestions' provides a concise summary of the draft guidance as well as recommendations for the healthcare community. (9 pages)
FY2015 Federal Information Security Modernization Act Report: Status of CSB's Information Security Program	EPA Office of Inspector General	January 27, 2016	The Chemical Safety Board, the government board that investigates industrial chemical accidents, does not keep track of computer systems it has outsourced to contractors, which could jeopardize information confidentiality. The audit criticizes the board for lacking a complete catalog of contractor-run systems, as well as databases maintained by other federal agencies. Data applications running in the cloud also have not been inventoried. (30 pages)
			The Obama Administration is creating a new organization within the Office of Personnel Management

The Way Forward for Federal Background Investigations	FBI	January 22, 2016	to handle background investigations, in its latest response to last year's revelations that hackers had pilfered highly sensitive documents on 22 million Americans. The new organization, the National Background Investigations Bureau, will be headed by a presidential appointee and will have a "considerable amount of operational autonomy." The technology systems will be "designed, built, secured, and operated" by the Defense Department.
Audit of NRC's Network Security Operations Center	Nuclear Regulatory Commission (NRC), Office of the Inspector General	January 11, 2016	According to the audit, security contracts related to unclassified nuclear computer systems do not specify who is responsible for protecting them from attacks. The NRC's Security Operations Center (SOC) is not "optimized to protect the agency's network in the current cyber treat environment." The report did not examine classified NRC networks. (18 pages)
DOT&E FY2015 Annual Report (Cybersecurity excerpt; click here for full report)	DOD Office of the Director, Operational Test and Evaluation	January 2016	Despite some key improvements from the previous fiscal year, Defense Department missions and systems remain vulnerable to hacking. Cyber testing teams deployed on DOD networks were "frequently in a position to deliver cyber effects that could degrade the performance of operational missions." (8 pages)
Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework	GAO	December 17, 2015	The Cybersecurity Enhancement Act of 2014 included provisions for GAO to review aspects of the cybersecurity standards and procedures developed by the National Information Standards and Technology (NIST). The report determines the extent to which (1) NIST facilitated the development of voluntary cybersecurity standards and procedures and (2) federal agencies promoted these standards and procedures. GAO examined NIST's efforts to develop standards, surveyed a non-generalizable sample of critical infrastructure stakeholders, reviewed agency documentation, and interviewed relevant officials. (48 pages)
Semiannual Report to the Congress: April 1, 2015 to September 30, 2015	Department of State, Office of Inspector General (OIG)	December 9, 2015	Between April and September 2015, a number of cybersecurity incidents illustrated deficiencies in the way State department personnel went about protecting networks. Malicious actors exploited vulnerabilities, compromised sensitive information, and caused significant downtime to normal business operations. (99 pages)
Department of Education and Other Federal Agencies Need to Better Implement Controls	GAO	November 17, 2015	Since 1997, GAO has identified federal information security as a government-wide high-risk area, and in February 2015, expanded this to include protecting the privacy of personally identifiable information (PII). This statement provides information on cyber threats facing federal systems and information security weaknesses identified at federal agencies, including the Department of Education. (27 pages)

Federal Agencies Need to Better Protect Sensitive Data	GAO	November 17, 2015	Over the past six years, GAO has made about 2,000 recommendations to improve information security programs and associated security controls. Agencies have implemented about 58% of these recommendations. Further, agency inspectors general have made a multitude of recommendations to assist their agencies. (22 pages)
Implementation of Reform Legislation Needed to Improve Acquisitions and Operations	GAO	November 4, 2015	The law commonly known as the Federal Information Technology Acquisition Reform Act (FITARA) was enacted in December 2014 and aims to improve federal information technology (IT) acquisition and operations. As GAO previously reported, underperformance of federal IT projects can be traced to a lack of disciplined and effective management and inadequate executive-level oversight. Last year, GAO added improving the management of IT acquisitions and operations to its high-risk listâ€”a list of agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation. (21 pages)
Inspector General's Statement Summarizing the Major Management and Performance Challenges Facing the U.S. Department of the Interior	Department of the Interior (DOI), OIG	November 2015	Networks at the Department of the Interior (DOI) were breached (nearly 20 times) over the past several years. An OIG report states, "hackers and foreign intelligence services have compromised DOI's computer networks by exploiting vulnerabilities in publicly accessible systems ... result[ing] in the loss of sensitive data and disruption of bureau operations." (Discussion of breaches starts on page 23.) (72 pages)
High-Risk Security Vulnerabilities Identified During Reviews of Information System General Controls at Three California Managed-Care Organizations Raise Concerns About the Integrity of Systems Used To Process Medicaid Claims	Health and Human Services (HHS), OIG	November 2015	Federal auditors found 74 high-risk security vulnerabilities in the IT systems of three California Medicaid-managed care organizations. The OIG found that most of these security vulnerabilities were "significant and pervasive" and potentially put Medicaid claims data at risk. The report raised concerns about the integrity of the systems used to process Medicaid-managed care claims.(19 pages)
Fiscal Year 2015 Top Management Challenges	Office of Personnel Management (OPM), OIG	October 30, 2015	See Internal Challenges section (pp. 10-19) for a discussion of challenges related to information technology, improper payments, the retirement claims process, and the procurement process. Officials in OPM's Office of Procurement Operations violated the Federal Acquisition Regulation and the agency's own policies in awarding a $20.7 million contract to provide credit monitoring and ID theft services. Investigators turned up "significant deficiencies" in the process of awarding the

			contract to Winvale Group and its subcontractor CSID. (22 pages)
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) the Federal Energy Regulatory Commission (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)
Agencies Need to Correct Weaknesses and Fully Implement Security Programs	GAO	September 29, 2015	Persistent weaknesses at 24 federal agencies illustrate the challenges they face in effectively applying information security policies and practices. The deficiencies place critical information and information systems used to support the operations, assets, and federal personnel at risk, and can impair agencies' efforts to fully implement effective information security programs. In prior reports, GAO and inspectors general have made hundreds of recommendations to agencies addressing deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain unimplemented. (71 pages)
Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses	GAO	September 24, 2015	DOD's Office of Small Business Programs (OSBP) has explored some options, such as online training videos, to integrate cybersecurity into its existing efforts; however, as of July 2015, the office had not identified and disseminated cybersecurity resources in its outreach and education efforts to defense small businesses. Although DOD OSBP is not required to educate small businesses on cybersecurity, its officials acknowledged that cybersecurity is an important and timely issue for small businesses. (32 pages)
Records: Energy Department Struck by Cyber Attacks	*USA Today* Review of Department of Energy Records	September 11, 2015	According to information obtained by *USA Today* through a Freedom of Information Act (FOIA) request, the Department of Energy's computer systems were breached by attackers more than 150 times between 2010 and 2014. Although there were many failed attempts to break into the systems, the success rate was roughly 15%.
The Centers for Medicare & Medicaid Services' Implementation of Security Controls Over the Multidimensional	HHS, OIG	September 2015	HealthCare.gov relies on a $110 million digital repository called MIDAS to store the information it collects. While MIDAS does not handle medical records, it does store names, Social Security numbers, addresses, passport numbers, and financial and employment information for exchange customers. In addition to poor security policies, the HHS audit found 135 database

Insurance Data Analytics System Needs Improvement			vulnerabilitiesâ€”such as software bugsâ€”22 of which were classified as "high risk." (7 pages)
Information Security Concerns	Department of Labor (DOL), OIG	July 31, 2015	Report asserts that DOL only recently turned its attention to implementing two-factor authentication agency-wide in response to data breaches at OPM. It also detailed lingering problems with former employees and contractors having privileged access to government systems. (16 pages)
Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning	GAO	July 23, 2015	The report addresses (1) whether threats and hazards have caused utility disruptions on DOD installations and, if so, what impacts they have had; (2) the extent to which DOD's collection and reporting on utility disruptions is comprehensive and accurate; and (3) the extent to which DOD has taken actions and developed and implemented guidance to mitigate risks to operations at its installations in the event of utility disruptions. (72 pages)
U.S. Postal Service Cybersecurity Functions	U.S. Postal Service (USPS), OIG	July 17, 2015	The report found that Postal Service leadership had not fostered a culture of effective cybersecurity across the enterprise. Staffing and resources for cybersecurity functions focused heavily on complying with specific legal and industry requirements, leaving limited resources for systems that are not subject to these requirements. In addition, management had not integrated cybersecurity risks into a comprehensive cybersecurity strategy. (41 pages)
Cyberthreats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies	GAO	July 8, 2015	This statement summarizes (1) cyberthreats to federal systems, (2) challenges facing federal agencies in securing their systems and information, and (3) government-wide initiatives aimed at improving cybersecurity. In preparing this statement, GAO relied on its previously published and ongoing work in this area. In previous work, GAO and agency IGs have made hundreds of recommendations to assist agencies in addressing cybersecurity challenges. GAO has also made recommendations to improve government-wide initiatives. (25 pages)
Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative	Federal Bureau of Investigation (FBI)	July 2015	Following the Office of the Inspector General's (OIG) April 2011 report on the FBI's ability to address the national cyber intrusion threat, in October 2012 the FBI launched its Next Generation Cyber (Next Gen Cyber) Initiative to enhance its ability to address cybersecurity threats to the United States. The objective of this audit was to evaluate the FBI's implementation of its Next Gen Cyber Initiative. (40 pages)
Recent Data Breaches Illustrate Need for Strong	GAO	June 24,	This statement summarizes (1) challenges facing federal agencies in securing their systems and information and (2) government-wide initiatives, including those led by

Controls across Federal Agencies		2015	DHS, aimed at improving cybersecurity. In preparing this statement, GAO relied on its previously published and ongoing work in this area. (17 pages)
Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems	GAO	June 2, 2015	DOD components have identified technical and policy changes to help protect classified information and systems from insider threats, but DOD is not consistently collecting this information to support management and oversight responsibilities. According to Office of the Under Secretary of Defense for Intelligence officials, they do not consistently collect this information because DOD has not identified a program office that is focused on overseeing the insider-threat program. Without an identified program office dedicated to oversight of insider-threat programs, DOD may not be able to ensure the collection of all needed information and could face challenges in establishing goals and in recommending resources and improvements to address insider threats. This is an unclassified version of a classified report GAO issued in April 2015. (55 pages)
Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems	GAO	April 22, 2015	Because of the risk posed by certain cyberthreats, it is crucial that the federal government take appropriate steps to secure its information and information systems. Until agencies take actions to address these challengesâ€"including the hundreds of recommendations GAO and inspectors general madeâ€"their systems and information will be at increased risk of compromise from cyber-based attacks and other threats. (21 pages)
Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen	GAO	April 14, 2015	GAO reviewed the Federal Aviation Administration's (FAA's) cybersecurity efforts. The report (1) identifies the cybersecurity challenges facing FAA as it shifts to the Next Generation Air Transportation System (NextGen) and how FAA has begun addressing those challenges, and (2) assesses the extent to which FAA and its contractors, in the acquisition of NextGen programs, have followed federal guidelines for incorporating cybersecurity controls. (56 pages)
FDIC Implemented Many Controls over Financial Systems, but Opportunities for Improvement Remain	GAO	April 9, 2015	The Federal Deposit Insurance Corporation (FDIC) has implemented numerous information security controls intended to protect its key financial systems; nevertheless, weaknesses remain that place the confidentiality, integrity, and availability of financial systems and information at risk. In 2014, the corporation implemented 27 of the 36 GAO recommendations pertaining to previously reported security weaknesses that were unaddressed as of December 31, 2013; actions to implement the remaining 9 recommendations are in progress. (28 pages)
			The Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers (PwC) to

Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2013	HHS, OIG	April 2015	evaluate information security programs at the Medicare administrative contractors (MACs), fiscal intermediaries, and carriers using a set of agreed-upon procedures. Some MACs have made improvements in their information security programs, but most still have a way to go in closing a number of key gaps. Among the concerns cited in the report are a lack of policies and procedures to reduce risk, failure to conduct periodic testing of information security controls, and insufficient incident detection reporting and response. (19 pages)
The FBI: Protecting the Homeland in the 21st Century	9/11 Review Commission	March 26, 2015	The 9/11 Review Commission found in its report on the FBI and its modern national security mission that while the FBI and DHS' relationship has improved in the past few years, especially on counterterrorism, that improvement has lagged in the area of cybersecurity. "The challenge for both DHS and the FBI in coordinating cyber relationships is due in large part to the lack of clarity at the national level on cyber roles and responsibilities," the commissioners wrote. "While Washington tries to coordinate the overlapping responsibilities of various federal agencies, the private sector is left in the dark. â€¦ The FBI is limited in its cyber efforts by the muddled national cyber architecture that will continue to affect the relationship with DHS. This issue â€¦ is beyond the FBI's ability to address in isolation." (128 pages)
Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data	GAO	March 19, 2015	Until the Internal Revenue Service (IRS) takes additional steps to (1) address unresolved and newly identified control deficiencies and (2) effectively implement elements of its information security program, including updating policies, test and evaluation procedures, and remedial action procedures, its financial and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification, or disclosure. GAO recommends that IRS take five additional actions to more effectively implement elements of its information security program. In a separate report with limited distribution, GAO recommends 14 actions that IRS can take to address newly identified control weaknesses. (30 pages)
Healthcare.gov: CMS Has Taken Steps to Address Problems, but Needs to Further Implement Systems Development Best	GAO	March 4, 2015	GAO reviewed CMS's management of the development of IT systems supporting the federal marketplace. Its objectives were to (1) describe problems encountered in developing and deploying systems supporting Healthcare.gov and determine the status of efforts to address deficiencies and (2) determine the extent to which CMS applied disciplined practices for managing and overseeing the development effort, and the extent to which HHS and OMB provided oversight. GAO recommended that CMS take seven actions to implement

Practices			improvements in its requirements management, system testing, and project oversight, and that HHS improve its oversight of the Healthcare.gov effort. (86 pages)
High Risk List: Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information	GAO	February 11, 2015	If cyber assets are not adequately protected, it "could lead to serious consequences and result in substantial harm to individuals and to the federal government." The government still faces challenges in achieving that goal, however, in several areas, including establishing risk-based cybersecurity programs at federal agencies, securing the global IT supply chain, securing critical infrastructure, overseeing IT contractors, improving incident response, and putting security programs in place at small agencies.
DOT&E FY 2014 Annual Report (Director Of Operational Test & Evaluation)	DOD Office of the Director, Operational Test and Evaluation (OT&E)	January 2015	A series of live fire tests of the military's computer networks security in 2015 found many combatant commands could be compromised by low-to-middling skilled hackers and might not be able to "fight through" in the face of enemy cyberattacks. The assessment echoes previous OT&E annual assessments, which routinely found that military services and combatant commands did not have a sufficiently robust security posture or training to repel sustained cyberattacks during battle. (91 pages)
A Review of the U.S. Navy Cyber Defense Capabilities: Abbreviated Version of a Classified Report	National Research Council (NRC)	January 2015	The NRC appointed an expert committee to review the U.S. Navy's cyber defense capabilities. The Department of the Navy determined that the committee's final report is classified in its entirety under Executive Order 13526 and therefore cannot be made available to the public. A Review of U.S. Navy Cyber Defense Capabilities, the abbreviated report, provides background information on the full report and the committee that prepared it. (13 pages)
Final Audit Report: Federal Information Security Management Act Audit FY 2014	Office of Personnel Management (OPM)	November 12, 2014	OPM's OIG reported that the agency "does not maintain a comprehensive inventory of servers, databases, and network devices." The report also noted that eleven "major systems" were operating without the agency certifying they met security standards. (66 pages)
FFIEC Cybersecurity Assessment: General Observations	Federal Financial Institutions Examination Council (FFIEC)	November 3, 2014	Companies are critically dependent on IT. Financial companies should routinely scan IT networks for vulnerabilities and anomalous activities and test systems for potential exposure to cyberattacks. The study recommends sharing threat data through such avenues as the Financial Services Information Sharing and Analysis Center.
Healthcare.gov: Information Security			The specific objectives of this work were to (1) describe the planned exchanges of information between the Healthcare.gov website and other organizations and (2)

and Privacy Controls Should Be Enhanced to Address Weaknesses	GAO	September 18, 2014	assess the effectiveness of programs and controls CMS implemented to protect the security and privacy of the information and IT systems supporting Healthcare.gov. Although CMS has security and privacy protections in place for Healthcare.gov and related systems, weaknesses exist that put these systems and the sensitive personal information they contain at risk. (17 pages)
FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain	GAO	July 17, 2014	FDIC has implemented numerous information security controls intended to protect its key financial systems; nevertheless, weaknesses place the confidentiality, integrity, and availability of financial systems and information at unnecessary risk. In 2013, the corporation implemented 28 of the 39 open GAO recommendations pertaining to previously reported security weaknesses that were unaddressed as of December 31, 2012. (30 pages)
Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity	GAO	June 5, 2014	GAO's objective was to identify the extent to which DHS and other stakeholders have taken steps to address cybersecurity in the maritime port environment. GAO examined relevant laws and regulations, analyzed federal cybersecurity-related policies and plans, observed operations at three U.S. ports selected based on being a high-risk port and a leader in calls by vessel type (e.g., container), and interviewed federal and nonfederal officials. (54 pages)
HHS Activities to Enhance Cybersecurity	HHS	May 12, 2014	Additional oversight on cybersecurity issues from outside of HHS is not necessary, according to an HHS report on its existing cyber regulatory policies. "All of the regulatory programs identified [in the HHS Section 10(a) analysis] operate within particular segments of the [Healthcare and Public Health] Sector. Expanding any or each of these authorities solely to address cybersecurity issues would not be appropriate or recommended."
Inadequate Practice and Management Hinder Department's Incident Detection and Response	Department of Commerce (DOC) OIG	April 24, 2014	Auditors sent a prolonged stream of deliberately suspicious network traffic to five public-facing websites at the DOC to assess incident-detection capabilities. Only one bureauâ€”auditors do not say whichâ€”successfully moved to block the suspicious traffic. Responses at the other bureaus ranged from no action to ineffective action, even for those that paid for special security services from vendors. (15 pages)
IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk	GAO	April 8, 2014	"Until the Internal Revenue Service (IRS) takes additional steps to (1) more effectively implement its testing and monitoring capabilities, (2) ensure that policies and procedures are updated, and (3) address unresolved and newly identified control deficiencies, its financial and taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure. These deficiencies, including shortcomings in

			the information security program, indicate that IRS had a significant deficiency in its internal control over its financial reporting systems for FY2013." (29 pages)
High-Risk Security Vulnerabilities Identified During Reviews of Information Technology General Controls at State Medicaid Agencies	HHS OIG	March 2014	The report says dozens of high-risk security vulnerabilities found in information systems at 10 state Medicaid agencies should serve as a warning to other states about the need to take action to prevent fraud.
Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent	GAO	December 9, 2013	GAO recommends that "to improve the consistency and effectiveness of governmentwide data breach response programs, the Director of OMB should update its guidance on federal agencies' responses to a PII-related data breach to include (1) guidance on notifying affected individuals based on a determination of the level of risk; (2) criteria for determining whether to offer assistance such as credit monitoring to affected individuals; and (3) revised reporting requirements for PII-related breaches to US-CERT [Computer Emergency Response Team], including time frames that better reflect the needs of individual agencies and the government as a whole and consolidated reporting of incidents that pose limited risk." (67 pages)
The Department of Energy's July 2013 Cyber Security Breach	DOE OIG	December 2013	Nearly eight times as many current and former DOE staff members were affected by a July 2013 computer hack than was previously estimated, according to the agency's inspector general. 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)
GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be EnhancedÂ	GAO	November 6, 2013	GAO was reviewed the effects of global positioning system (GPS) disruptions on the nation's critical infrastructure. GAO examined (1) the extent to which DHS has assessed the risks and potential effects of GPS disruptions on critical infrastructure; (2) the extent to which the Department of Transportation (DOT) and DHS have developed backup strategies to mitigate GPS disruptions; and (3) what strategies, if any, selected critical infrastructure sectors employ to mitigate GPS disruptions and any remaining challenges. (58 pages)
Federal Energy Regulatory Commission's	DOE OIG	October	To help protect against continuing cybersecurity threats, the commission estimated that it would spend approximately $5.8 million during FY2013 to secure its information technology assets, a 9% increase compared with FY2012.... As directed by FISMA, the OIG

Unclassified Cyber Security Program - 2013		2013	conducted an independent evaluation of the commission's unclassified cybersecurity program to determine whether it adequately protected data and information systems. The report presents the results of the evaluation for FY2013. (13 pages)
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts	GAO	September 17, 2013	Within DHS, one in five jobs at a key cybersecurity component is vacant, in large part due to steep competition in recruiting and hiring qualified personnel.Â National Protection and Programs Directorate (NPPD) officials cited challenges in recruiting cyber professionals because of the length of time taken to conduct security checks to grant top-secret security clearances as well as low pay in comparison with the private sector. (47 pages)
Offensive Cyber Capabilities at the Operational Level: The Way Ahead	Center for Strategic and International Studies (CSIS)	September 16, 2013	The report examines whether DOD should make a more deliberate effort to explore the potential of offensive cyber tools at levels below that of a combatant command. (20 pages)
An Assessment of the Department of Defense Strategy for Operating in Cyberspace	U.S. Army War College	September 2013	This monograph is organized in three main parts. The first part explores the evolution of cyberspace strategy through a series of government publications leading up to the *DoD Strategy for Operating in Cyberspace*. The second part elaborates on and critiques each strategic initiative in terms of significance, novelty, and practicality. The third part critiques DOD's strategy as a whole. (60 pages)
Joint Professional Military Education Institutions in an Age of Cyber Threat	Francesca Spidalieri (Pell Center Fellow)	August 7, 2013	The report found that the Joint Professional Military Education at the six U.S. military graduate schoolsâ€”a requirement for becoming a joint staff officer and for promotion to the senior ranksâ€”has not effectively incorporated cybersecurity into specific courses, conferences, war-gaming exercises, or other forms of training for military officers. Although these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists. (18 pages)
Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment	GAO	May 21, 2013	The federal government began efforts to address supply chain security for commercial networks. A variety of other approaches exist for addressing the potential risks posed by foreign-manufactured equipment in commercial communications networks, including 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 chooses to pursue such approaches. (52 pages)
			Until DHS and its sector partners develop appropriate

Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts	GAO	April 11, 2013	outcome-oriented metrics, it will be difficult to gauge the effectiveness of efforts to protect the nation's core and access communications networks and critical support components of the Internet from cyber incidents. Although no cyber incidents affecting the nation's core and access networks have been reported, communications networks operators can use FCC's and DHS's reporting mechanisms to share information on outages and incidents. (45 pages)
Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities	GAO	April 4, 2013	Agencies have neither held entities accountable for coordinating nor assessed opportunities for further enhancing coordination to help reduce the potential for overlap and achieve efficiencies. The Department of Justice (DOJ), DHS, and the Office of National Drug Control Policy (ONDCP)â€”the federal agencies that oversee or provide support to the five types of field-based entitiesâ€”acknowledged that it is important for entities to work together and share information, but these agencies do not hold the entities accountable for such coordination. (72 pages)
Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges	GAO	March 7, 2013	"[A]lthough federal law assigns the Office of Management and Budget (OMB) responsibility for oversight of federal government information security, OMB recently transferred several of these responsibilities to Department of Homeland Security (DHS).... [I]t remains unclear how OMB and Department of Homeland Security are to share oversight of individual departments and agencies. Additional legislation could clarify these responsibilities." (36 pages)
Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented	GAO	February 14, 2013	GAO recommends that the White House cybersecurity coordinator develop an overarching federal cybersecurity strategy that includes all key elements of the desirable characteristics of a national strategy. Such a strategy would provide a more effective framework for implementing cybersecurity activities and better ensure that such activities will lead to progress in cybersecurity. (112 pages)
Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project	GAO	January 25, 2013	The Federal Communications Commission (FCC) did not effectively implement appropriate information security controls in the initial components of the Enhanced Secured Network (ESN) project. Weaknesses identified in the commission's deployment of ESN's project components as of August 2012 resulted in unnecessary risk that sensitive information could be disclosed, modified, or obtained without authorization. GAO is made seven recommendations to the FCC to implement management controls to help ensure that ESN meets its objective of securing FCC's systems and information. (35 pages)

Follow-up Audit of the Department's Cyber Security Incident Management Program	DOE OIG	December 2012	In 2008, the DOE's Cyber Security Incident Management Program (DOE/IG-0787, January 2008) reported the Department and National Nuclear Security Administration (NNSA) had established and maintained a number of independent, at least partially duplicative, cybersecurity incident management capabilities. Several issues were identified that limited the efficiency and effectiveness of the department's cybersecurity program and adversely affected the ability of law enforcement to investigate incidents. In response to the findings, management concurred with the recommendations and indicated that it had initiated actions to address the issues. (25 pages)
Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned	GAO	July 11, 2012	GAO recommended that the Secretaries of Agriculture, Health and Human Services, Homeland Security, State, and the Treasury, and the Administrators of the General Services Administration (GSA) and Small Business Administration (SBA) should direct their respective chief information officers to establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed the report, as applicable. (43 pages)
Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight	GAO	July 9, 2012	DOD's oversight of electronic warfare capabilities may be further complicated by its evolving relationship with computer network operations, which is also an information operations-related capability. Without clearly defined roles and responsibilities and updated guidance regarding oversight responsibilities, DOD does not have reasonable assurance that its management structures will provide effective department-wide leadership for electronic warfare activities and capabilities development and ensure effective and efficient use of its resources. (46 pages)
Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage	GAO	June 28, 2012	The statement discusses (1) cyber threats facing the nation's systems, (2) reported cyber incidents and their impacts, (3) security controls and other techniques available for reducing risk, and (4) the responsibilities of key federal entities in support of protecting Internet protocol. (20 pages)
Cyber Sentries: Preparing Defenders to Win in a Contested Domain	Army War College	February 7, 2012	The paper examines the current impediments to effective cybersecurity workforce preparation and offers new concepts to create Cyber Sentries through realistic training, network authorities tied to certification, and ethical training. These actions present an opportunity to significantly enhance workforce quality and allow DOD to operate effectively in the contested cyber domain in accordance with the vision established in its Strategy for Cyberspace Operations. (38 pages)
			According to the DOE' inspector general, the

The Department's Management of the Smart Grid Investment Grant Program	DOE OIG	January 20, 2012	department's rush to award stimulus grants for projects under the next generation of the power grid, known as the Smart Grid, resulted in some firms receiving funds without submitting complete plans for how to safeguard the grid from cyberattacks. (21 pages)
Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination	GAO	November 29, 2011	To ensure that government-wide cybersecurity workforce initiatives are better coordinated and planned, and to better assist federal agencies in defining roles, responsibilities, skills, and competencies for their workforce, the DOC Secretary, OMB Director, OPM, and DHS Secretary should collaborate through the National Initiative for Cybersecurity Education (NICE) initiative to develop and finalize detailed plans allowing agency accountability, measurement of progress, and determination of resources to accomplish agreed-upon activities. (86 pages)
Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management	GAO	October 17, 2011	GAO recommended that the OMB update its guidance to establish measures of accountability for ensuring that chief information officers' responsibilities are fully implemented and to require agencies to establish internal processes for documenting lessons learned. (72 pages)
Information Security: Additional Guidance Needed to Address Cloud Computing Concerns	GAO	October 6, 2011	Twenty-two of 24 major federal agencies reported that they were either concerned or very concerned about the potential information security risks associated with cloud computing. GAO recommended that the NIST issue guidance specific to cloud computing security. (17 pages)
Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements	GAO	October 3, 2011	Weaknesses in information security policies and practices at 24 major federal agencies continue to place the confidentiality, integrity, and availability of sensitive information and information systems at risk. Consistent with this risk, reports of security incidents from federal agencies are on the rise, increasing by more than 650% over the past five years. Each of the 24 agencies reviewed had weaknesses in information security controls. (49 pages)
Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates	GAO	July 29, 2011	The letter discusses DOD's cyber and information assurance budget for FY2012 and future years' defense spending. The objectives of the review were to (1) assess the extent to which DOD prepared an overarching budget estimate for full-spectrum cyberspace operations across the department and (2) identify the challenges DOD faced in providing such estimates. (33 pages)

Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities	GAO	July 25, 2011	GAO recommended that DOD evaluate how it is organized to address cybersecurity threats; assess the extent to which it developed joint doctrine that addresses cyberspace operations; examine how it assigns command and control responsibilities; and determine how it identifies and acts to mitigate key capability gaps involving cyberspace operations. (79 pages)
Information Security: [Department of] State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain	GAO	July 8, 2011	The Department of State implemented a custom application called iPost and a risk-scoring program that aimed to provide continuous monitoring capabilities of information security risk to elements of the department's IT infrastructure. To improve implementation of iPost at State, the Secretary of State directed the chief information officer to develop, document, and maintain an iPost configuration management and test process. (63 pages)
USCYBERCOM [U.S. Cyber Command] and Cyber Security: Is a Comprehensive Strategy Possible?	Army War College	May 12, 2011	Examines five aspects of USCYBERCOM: (1) organization, (2) command and control, (3) computer network operations, (4) synchronization, and (5) resourcing. Identifies areas that currently present significant risk to USCYBERCOM's ability to create a strategy that can achieve success in its cyberspace operations and recommends potential solutions that can increase the effectiveness of the USCYBERCOM strategy. (32 pages)
Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats	GAO	March 16, 2011	The White House, OMB, and certain federal agencies have undertaken several government-wide initiatives intended to enhance information security at federal agencies. Although progress has been made on these initiatives, they all face challenges that require sustained attention, and GAO has made several recommendations for improving the implementation and effectiveness of these initiatives. (15 pages)
Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security	DOE OIG	January 26, 2011	The Nuclear Energy Regulatory Commission (NERC) developed Critical Infrastructure Protection (CIP) cybersecurity reliability standards, which were approved by the Federal Energy Regulatory Commission (FERC) in January 2008. Although the commission had taken steps to ensure CIP cybersecurity standards were developed and approved, NERC's testing revealed that such standards did not always include controls commonly recommended for protecting critical information systems. In addition, the CIP standards implementation approach and schedule approved by the commission were not adequate to ensure that systems-related risks to the nation's power grid were mitigated or addressed in a timely manner. (30 pages)
Information Security: Federal			Existing government-wide guidelines and oversight

Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk	GAO	November 30, 2010	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 attacks. (50 pages)
DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened	GAO	September 23, 2010	DHS has not developed an effective way to ensure that critical national infrastructure, such as electrical grids and telecommunications networks, can bounce back from a disaster. DHS has conducted surveys and vulnerability assessments of critical infrastructure to identify gaps, but has not developed a way to measure whether owners and operators of that infrastructure adopt measures to reduce risks. (46 pages)
Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems	GAO	September 15, 2010	OMB and NIST established policies and guidance for civilian non-national security systems, and other organizations, including the Committee on National Security Systems (CNSS), DOD, and the U.S. intelligence community, and have developed policies and guidance for national security systems. GAO assessed the progress of federal efforts to harmonize policies and guidance for these two types of systems. (38 pages)
Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats	GAO	June 16, 2010	GAO and agency IGs have made hundreds of recommendations over the past several years, many of which agencies are implementing. In addition, the White House, OMB, and certain federal agencies have undertaken several government-wide initiatives intended to enhance information security at federal agencies. Progress has been made on these initiatives, but they all face challenges that require sustained attention. GAO made several recommendations for improving the implementation and effectiveness of these existing initiatives. (15 pages)
NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses	DOE, Idaho National Laboratory	May 2010	The National SCADA Test Bed (NSTB) program reported 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)
Information Security: Concerted Response Needed to Resolve Persistent Weaknesses	GAO	March 24, 2010	Without proper safeguards, federal computer systems are vulnerable to malicious intruders seeking to obtain sensitive information. The need for a vigilant approach to information security is demonstrated by the pervasive and sustained cyberattacks against the United States; these attacks continue to pose a potentially devastating impact to systems and the operations and critical infrastructures they support. (21 pages)

Cybersecurity: Progress Made But Challenges Remain in Defining and Coordinating the Comprehensive National Initiative	GAO	March 5, 2010	To address strategic challenges in areas that are not the subject of the Comprehensive National Cybersecurity Initiative's existing projects but remain key to achieving the initiative's overall goal of securing federal information systems, GAO recommended that OMB's director continue developing a strategic approach to identity management and authentication and link it to the Homeland Security Presidential Directive 12. The directive was initially described in the Chief Information Officers Council's (CIOC's) plan to implement federal identity, credential, and access management to provide greater assurance that only authorized individuals and entities can gain access to federal information systems. (64 pages)
Continued Efforts Are Needed to Protect Information Systems from Evolving Threats	GAO	November 17, 2009	GAO identified weaknesses in all major categories of information security controls at federal agencies. For example, in FY2008, weaknesses were reported in such controls at 23 of 24 major agencies. Specifically, agencies did not consistently authenticate users to prevent unauthorized access to systems; apply encryption to protect sensitive data; or log, audit, and monitor security-relevant events, among other actions. (24 pages)
Efforts to Improve Information Sharing Need to Be Strengthened	GAO	August 27, 2003	Information on threats, methods, and techniques of terrorists is not routinely shared, and the information that is shared is not perceived as timely, accurate, or relevant. (59 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are web pages.

Table 4. Federal Workforce

(includes evaluations, grants, job programs, surveys, and statistics on federal cybersecurity personnel)

Title	Source	Date	Notes
Information Assurance Scholarship Program	DOD	Continuously Updated	The Information Assurance Scholarship Program is designed to increase the number of qualified personnel entering the information assurance and technology fields within DOD. The scholarships also are an attempt to effectively retain military and civilian cybersecurity and IT personnel.
U.S. Digital Services	White House	Continuously Updated	The U.S. Digital Services (USDS) is a group of about 100 technologists on two- to four-year fellowships that do some cybersecurity work. Cybersecurity is only a small portion of USDS' work, however, and the group is not yet spread throughout all agencies.
PERSEREC (Personnel and	DOD	Continuously	The Pentagon is expected to create a database for investigating the trustworthiness of personnel who could have access to federal facilities and computer systems. The Defense

Security Research Center)		Updated	Information System for Security, or DISS, will consolidate two existing tools used for vetting employees and job applicants.
NIST 'RAMPS' Up Cybersecurity Education and Workforce Development With New Grants	NIST	May 12, 2016	NIST is offering up to $1 million in grants to establish up to eight Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development. Applicants must be nonprofit organizations, including institutions of higher education, located in the United States or its territories. Applicants must also demonstrate through letters of interest that at least one of each of the following types of organizations is interested in being part of the proposed regional alliance: K-12 school or Local Education Agency (LEA), institution of higher education or college/university system, and a local employer.
Closing Skills Gaps: Strategy, Reporting and Monitoring	OPM	April 15, 2016	OPM "revalidated" the need to close skills gaps in certain "high-risk mission critical occupations," including cybersecurity, acquisition, and STEM. Agency experts and chief human capital officers will work together to develop a governmentwide strategy "to address the root causes for why an occupation has been deemed 'at risk.'" OPM tasked chief human capital officers with identifying specific skills gaps in their agencies. The memo calls on agencies to develop 4-year and 10-year plans for closing gaps in those areas.
The Way Forward for Federal Background Investigations	FBI	January 22, 2016	The Obama Administration is creating a new organization within the OPM to handle background investigations, in its latest response to last year's revelations that hackers had pilfered highly sensitive documents on 22 million Americans. The new organization, the National Background Investigations Bureau, will be headed by a presidential appointee, and will have a "considerable amount of operational autonomy." The technology systems will be "designed, built, secured, and operated" by the Defense Department.
Guidance on recruitment, relocation and retention (3R) incentives	OPM	January 15, 2016	OPM has enhanced the ability of federal human resources managers to use recruitment, relocation, and retention (3R) incentives to attract or hang onto cybersecurity workers. The more flexible grants for exceptions to the 3R spending limit "may assist agencies in recruiting and retaining the most highly qualified cybersecurity employees to meet the government's important challenges of strengthening federal networks, systems and data."
NIST to Support Cybersecurity Jobs "Heat Map" to Highlight Employer Needs and Worker Skills	NIST	October 27, 2015	NIST will fund a project developing a visualization tool to show the demand for and availability of cybersecurity jobs across the United States. CompTIA, a non-profit information technology trade association, in partnership with job market research and analytics company Burning Glass Technologies, received a three-year grant to create a "heat map" visualizing the need for and the supply of cybersecurity professionals across the country.
Workforce Shortfall Due to Hiring			In 2014, the average annual salary of a federal cybersecurity worker was $110,500, with federal contractors taking home

[Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction]	(ISC)^2	April 17, 2015	$114,000. U.S. private-sector cyber professionals are expected to bring in $118,000 in 2015. Analysts from Frost & Sullivan forecast a shortfall of 1.5 million cyber professionals by 2020. This number is compounded by 45% of hiring managers reporting that they are struggling to support additional hiring needs and 62% of respondents reporting that their organizations have too few information security professionals. (46 pages)
Tech Hire	White House	March 9, 2015	The White House has unveiled a multi-sector effort to empower Americans with technology skills. Many jobs do not require a four-year computer science degree. To kick off TechHire, 21 regions, with more than 120,000 open technology jobs and more than 300 employer partners in need of this workforce, are announcing plans to work together to find new ways to recruit and place applicants based on their actual skills and to create more fast-track tech training opportunities.
U.S. Dept. of Energy to Offer $25M Grant for Cybersecurity	Department of Energy (DOE)	January 15, 2015	DOE announced a $25 million cybersecurity education grant over five years to establish a Cybersecurity Workforce Pipeline Consortium within the DOE with funding from its Minority Serving Institutions Partnerships Program under its National Nuclear Security Administration. The participants are historically black colleges and universities, national labs, and K-12 school districts.
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts	GAO	September 17, 2013	Within DHS, one in five jobs at a key cybersecurity component is vacant, in large part due to steep competition in recruiting and hiring qualified personnel.Â National Protection and Programs Directorate officials cited challenges in recruiting cyber professionals because of the length of time taken to conduct security checks to grant top-secret security clearances and low pay in comparison with the private sector. (47 pages)
Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making	National Academies Press	September 16, 2013	The report "examines workforce requirements for cybersecurity; the segments and job functions in which professionalization is most needed; the role of assessment tools, certification, licensing, and other means for assessing and enhancing professionalization; and emerging approaches, such as performance-based measures. It also examines requirements for the federal (military and civilian) workforce, the private sector, and state and local government." (66 pages)
Joint Professional Military Education Institutions in an Age of Cyber Threat	Francesca Spidalieri (Pell Center Fellow)	August 7, 2013	The report found that the Joint Professional Military Education at the six U.S. military graduate schoolsâ€"a requirement for becoming a joint staff officer and for promotion to the senior ranksâ€"has not effectively incorporated cybersecurity into specific courses, conferences, war-gaming exercises, or other forms of training for military officers. Although these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists. (18 pages)

Special Cybersecurity Workforce Project (Memo for Heads of Executive Departments and Agencies)	OPM	July 8, 2013	OPM is collaborating with the White House Office of Science and Technology Policy, the Chief Human Capital Officers Council, and the Chief Information Officers Council in implementing a special workforce project that tasks federal agencies' cybersecurity, information technology, and human resources communities to build a statistical data set of existing and future cybersecurity positions in the OPM Enterprise Human Resources Integration data warehouse.
Global Information Security Workforce Study	(ISC)^2 Foundation and Frost and Sullivan	May 7, 2013	Federal cyber workers earn an average salary of $106,430, less than the average private-sector salary of $111,376. The lag in federal salaries is likely due to federal budget restraints. (28 pages)
2012 Information Technology Workforce Assessment for Cybersecurity	Department of Homeland Security (DHS)	March 14, 2013	The report, which is based on an anonymous survey of nearly 23,000 cyber workers across 52 departments and agencies, found that while the majority (49%) of cyber federal workers has more than 10 years of service until they reach retirement eligibility, nearly 33% will be eligible to retire in the next three years. (131 pages)
CyberSkills Task Force Report	DHS	October 2012	DHS's task force on CyberSkills proposes far-reaching improvements to enable the department to recruit and retain the cybersecurity talent it needs. (41 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 develops a measurement model used to guide curriculum, assessments, and other development of technical and operational Smart-Grid cybersecurity knowledge, skills, and abilities. (178 pages)
Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination	GAO	November 29, 2011	To ensure that government-wide cybersecurity workforce initiatives are better coordinated and planned, and to better assist federal agencies in defining roles, responsibilities, skills, and competencies for their workforce, the Secretaries of Commerce and Homeland Security and the Directors of OMB and OPM collaborated through the National Initiative for Cybersecurity Education (NICE) initiative to develop and finalize detailed plans allowing agency accountability, measurement of progress, and determination of resources to accomplish agreed-upon activities. (86 pages)
Cyber Operations Personnel Report	DOD	April 2011	The report focuses on FY2009 DOD Cyber Operations personnel, with duties and responsibilities as defined in Section 934 of the FY2010 National Defense Authorization Act (NDAA). Its appendices include the following: Appendix Aâ€”Cyber Operations-Related Military Occupations Appendix Bâ€”Commercial Certifications Supporting the DOD Information Assurance Workforce Improvement Program Appendix Câ€”Military Services Training and Development

			Appendix Dâ€”Geographic Location of National Centers of Academic Excellence in Information Assurance (84 pages)
The Power of People: Building an Integrated National Security Professional System for the 21st Century	Project on National Security Reform	November 2010	The study was conducted in fulfillment of Section 1054 of the FY2010 NDAA, which required the commissioning of a study by "an appropriate independent, nonprofit organization, of a system for career development and management of interagency national security professionals." (326 pages)

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are documents; other cited resources are web pages.

Table 5. White House and Office of Management and Budget

(reports by or about cybersecurity policies in the White House, OMB, or executive branch agencies)

Title	Source	Date	Notes
Improving Cybersecurity	OMB	Continuously Updated	OMB is working with agencies, inspectors general, chief information officers, and senior agency officials in charge of privacy, as well as the Government Accountability Office (GAO) and Congress, to strengthen the federal government's IT security and privacy programs. The site provides information on Cross-Agency Priority (CAP) goals, proposed cybersecurity legislation, CyberStat, continuous monitoring and remediation, using SmartCards for identity management, and standardizing security through configuration settings.
FACT SHEET: Announcing Over $80 million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative	White House	September 26, 2016	In September 2015, the White House launched the Smart Cities Initiative to make it easier for cities, federal agencies, universities, and the private sector to work together to research, develop, deploy, and testbed new technologies that can help make our cities more inhabitable, cleaner, and more equitable. This year, to kick off Smart Cities Week, the Administration is expanding this initiative, with more than $80 million in new federal investments and a doubling of the number of participating cities and communities, exceeding 70 in total.
Announcing the First Federal Chief Information Security Officer	White House	September 8, 2016	The Administration announced Brigadier General (retired) Gregory J. Touhill as the first Federal Chief Information Security Officer (CISO). A key feature of the Cybersecurity National Action Plan (CNAP) is the creation of the first CISO to drive cybersecurity policy, planning, and implementation across the federal government.

Revision of OMB Circular No. A-130, "Managing Information as a Strategic Resource"	OMB	July 28, 2016	OMB has revised Circular A-130, "Managing Information as a Strategic Resource," to reflect changes in law and advances in technology. The revisions also ensure consistency with executive orders, presidential directives, recent OMB policy, and National Institute of Standards and Technology standards and guidelines. The Circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the Federal information life cycle. (30 pages)
Letter Sent to 27 Executive Branch Offices Regarding Information Security Obligations Under the Federal Information Security Management Act (FISMA)	House Oversight and Government Reform Committee	July 26, 2016	The letter notes all agencies are required by law to submit annual reports to the committee and Office of Management and Budgetâ€”which is a part of EOPâ€”and that the term "agency" was intentionally defined broadly in the legislation, which specifically mentions EOP as an example. Requests a copy of EOP's FISMA report or, if it doesn't exist, an explanation of why the office is exempt. (17 pages)
Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response	OMB	July 1, 2016	OMB issued a memorandum to all department heads outlining how agencies should go about contracting for identity protection services. Going forward, all agencies offering identity protection services to citizens or employees must contract through the General Services Administration's Identity Monitoring Data Breach Response and Protection Services (IPS) blanket purchase agreement (BPA). (3 pages)
President Obama Appoints Commission on Enhancing National Cybersecurity	White House	April 13, 2016	President Barack Obama announced his intent to appoint individuals to the Commission on Enhancing National Cybersecurity.
Annual Report to Congress: Federal Information Security Modernization Act	OMB	March 18, 2016	In 2015, government agencies reported 77,183 cybersecurity incidents, a 10% increase from 69,851 incidents in 2014. These incidents were reported by government agencies to the United States Computer Emergency Readiness Team (US-CERT). Sixteen percent of these were caused by "non-cyber" reasons, such as employees losing data storage devices that contained personally identifiable information. [See p. 39 for agency scores]. (95 pages)
Cybersecurity		February 9,	The White House proposed a Cybersecurity National Action Plan, which provides a 35% increase in federal

National Action Plan	White House	2016	funds for the next budget year to boost the nation's ability to safeguard its computer networks, both private and public, from attacks while preserving privacy.
Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government	OMB	October 30, 2015	The document includes an update on the comprehensive review of the federal government's cyber policies, which took place during a 30-day "Cybersecurity Sprint" directed by the federal chief information officer in June 2015. The plan identifies a number of action items that the federal government will take in the coming year to improve the cybersecurity of the federal government networks. (21 pages)
Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements	OMB	October 30, 2015	The White House is updating annual cybersecurity guidelines that provide a definition for a "major" cyber incident. The new definition is mandated by a 2014 update to the Federal Information Security Management Act (FISMA). Agencies can consult with the Department of Homeland Security about whether an incident meets the major threshold, but ultimately it's up to the victim agency to make the final call. (11 pages)
Appendix III to OMB Circular No. A-130: Responsibilities for Protecting Federal Information Resources	OMB	October 21, 2015	The policy lays out guidance for managing IT investments, improving information security practices, and streamlining the process for acquiring new technology.
Strengthening & Enhancing Federal Cybersecurity for the 21st Century	OMB	August 3, 2015	In July 2015, OMB launched a 30-day Cybersecurity Sprint to assess and improve the health of all federal assets and networks, both civilian and military. As part of the Sprint, OMB directed agencies to further protect federal information, improve the resilience of their networks, and report on their successes and challenges. Agencies were instructed to immediately patch critical vulnerabilities, review and tightly limit the number of privileged users with access to authorized systems, and dramatically accelerate the use of strong authentication, especially for privileged users.
Request for Comments on Improving Cybersecurity Protections in Federal Acquisitions	OMB	July 30, 2015	OMB's Office of E-Government & Information Technology (E-Gov) is seeking public comment on draft guidance to improve cybersecurity protections in federal acquisitions. Threats to federal information systems have increased as agencies provide more services online and the demand to secure information on these systems increase. (1 page)
FACT SHEET: Administration	OMB	July 9, 2015	The 30-day Cybersecurity Sprint, by the Obama Administration in the wake of the OPM breach, has resulted in a jump in the use of multi-factor ID authentication and tens of thousands of scans of federal

Cybersecurity Efforts 2015			networks for vulnerabilities. The White House released a fact sheet detailing what the Administration has done to improve cybersecurity. (9 pages)
FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity	OMB	June 12, 2015	To further improve federal cybersecurity and protect systems against these evolving threats, the U.S. chief information officer (CIO) launched a 30-day Cybersecurity Sprint. The CIO instructed federal agencies to immediately take numerous steps to further protect federal information and assets and improve the resilience of federal networks. Agencies were instructed to immediately test networks for DHS-provided indicators, patch vulnerabilities flagged in weekly DHS scan reports, restrict the number of privileged user accounts and what they can do, and *dramatically* ramp up the use of multi-factor authentication, especially for sensitive users. On the latter three requirements, agencies were to report back to OMB and DHS on their progress within a month.
Management and Oversight of Information Technology Resources	OMB	June 10, 2015	The guidance takes major steps toward ensuring agency CIOs have significant involvement in procurement, workforce, and technology-related budget matters while continuing a partnership with other senior leaders. It also takes major steps toward positioning CIOs so that they can reasonably be held accountable for how effectively their agencies use modern digital approaches to achieve the objectives of effective and efficient programs and operations. (34 pages)
Policy to Require Secure Connections across Federal Websites and Web Services	OMB	June 8, 2015	In a memo to agency executives, federal CIO Tony Scott detailed four requirements for agencies to meet, starting with using a risk-based approach for determining which websites or web services to move to HTTPS first. Sites dealing with personally identifiable information (PII), where the content is sensitive, or where the site receives a high level of traffic should be migrated to HTTPS as soon as possible. Agencies have until Dec. 31, 2016, to move all public facing online services to the security standard. (5 pages)
White House Summit on Cybersecurity and Consumer Protection	White House	February 13, 2015	The Summit brought together leaders from across the country who have a stake in this issueâ€”industry, tech companies, law enforcement, consumer and privacy advocates, law professors who specialize in this field, and studentsâ€”to collaborate and explore partnerships that will help develop the best ways to bolster U.S. cybersecurity. Topics included Public-Private Collaboration on Cybersecurity; Improving Cybersecurity Practices at Consumer-Oriented Businesses and Organizations; Promoting More Secure Payment Technologies; Cybersecurity Information Sharing; International Law Enforcement Cooperation on

			Cybersecurity; Improving Authentication: Moving Beyond the Password; and Chief Security Officers' Perspectives: New Ideas on Technical Security.
Strengthening our Nation's Cyber Defenses (Announcing Plans for a New Cyber Threat Intelligence Integration Center)	White House	February 11, 2015	The White House will establish a new Cyber Threat Intelligence Integration Center, or CTIIC, under the auspices of the Director of National Intelligence. Currently, no single government entity is responsible for producing coordinated cyber threat assessments, and ensuring that information is shared rapidly among existing cyber centers and other elements within the government, and supporting the work of operators and policymakers with timely intelligence about the latest cyber threats and threat actors. The CTIIC is intended to fill these gaps.
National Security Strategy	White House	February 6, 2015	The document states the United States will "defend ourselves, consistent with U.S. and international law, against cyberattacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity." The strategy praises the NIST framework for cybersecurity and promises to work with Congress to "pursue a legislative framework that ensures high [cyber] standards" for critical infrastructure. The government will also work to develop "global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats." The document also promises to help other nations improve the cybersecurity of their critical infrastructure and develop laws that punish hackers. (32 pages)
Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices	OMB	October 3, 2014	OMB is making updates to streamline agency reporting of information security incidents to DHS's U.S. Computer Emergency Readiness Team (US-CERT) and to improve US-CERT's ability to respond effectively to information security incidents. Under the updates, losses of PII caused by non-electronic means must be reported within one hour of a confirmed breach to the agency privacy office rather than to US-CERT. (17 pages)
Assessing Cybersecurity Regulations	White House	May 22, 2014	The White House directed federal agencies to examine their regulatory authority over private-sector cybersecurity in the February 2013 executive order that also created the National Institute of Standards and Technology (NIST) cybersecurity framework. A review of agency reports concluded that "existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks." No new federal regulations are needed for improving the cybersecurity of privately held American critical infrastructure.
			The 24 largest federal departments and agencies spent $10.34 billion on cybersecurity in fiscal year 2014. The

Federal Information Security Management Act, Annual Report to Congress	OMB	May 1, 2014	Chief Financial Officers Act agency with the greatest expenditure was the DOD at $7.11 billion, followed by DHS at $1.11 billion. Federal agencies' collective request for cybersecurity spending during FY2015 amounts to about $13 billion, federal CIO Steven VanRoekel told reporters during the March rollout of the White House spending proposal for the coming fiscal yearâ€”making cybersecurity a rare area of federal information technology spending growth. (80 pages)
Big Data: Seizing Opportunities, Preserving Values	White House	May 2014	The findings outline a set of consumer protection recommendations, including that Congress should pass legislation on "single national data breach standard." (85 pages)
State and Local Government Cybersecurity	White House	April 2, 2014	The White House in March 2014 convened an array of stakeholders, including government representatives, local-government-focused associations, private-sector technology companies, and partners from multiple federal agencies at the State and Local Government Cybersecurity Framework Kickoff Event.
Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies	The President's Review Group on Intelligence and Communications Technologies	December 12, 2013	From the report, "The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future. These threats include international terrorism, the proliferation of weapons of mass destruction, and cyber espionage and warfare.... After careful consideration, we recommend a number of changes to our intelligence collection activities that will protect [privacy and civil liberties] values without undermining what we need to do to keep our nation safe." (308 pages)
Immediate Opportunities for Strengthening the Nation's Cybersecurity	President's Council of Advisors on Science and Technology (PCAST)	November 2013	The report recommends the government phase out insecure, outdated operating systems, such as Windows XP; implement better encryption technology; and encourage automatic security updates, among other changes. PCAST also recommends that the government help create cybersecurity best practices and audit their adoption in regulated industries. For independent agencies, PCAST proposes writing new rules that require businesses to report their cyber improvements. (31 pages)
Cross Agency Priority Goal: Cybersecurity, FY2013 Q3 Status Report	Performance.gov	October 2013	Executive branch departments and agencies achieved 95% implementation of the Administration's priority cybersecurity capabilities by the end of FY2014. These capabilities include strong authentication, Trusted Internet Connections (TIC), and continuous monitoring. (24 pages)
Incentives to Support Adoption		August 6,	From the report, "To promote cybersecurity practices and develop these core capabilities, we are working with critical infrastructure owners and operators to create a Cybersecurity Framework â€“ a set of core practices to

of the Cybersecurity Framework	White House	2013	develop capabilities to manage cybersecurity risk.... Over the next few months, agencies will examine these options in detail to determine which ones to adopt and how, based substantially on input from critical infrastructure stakeholders."
FY2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002	OMB	March 2013	More government programs violated data security law standards in 2012 than in the previous year. At the same time, computer security costs have increased by more than $1 billion. Inadequate training was a large part of the reason all-around scores for adherence to the Federal Information Security Management Act of 2002 (FISMA) slipped from 75% in 2011 to 74% in 2012. Agencies reported that about 88% of personnel with system access privileges received annual security awareness instruction, down from 99% in 2011. Meanwhile, personnel expenses accounted for the vast majorityâ€"90%â€"of the $14.6 billion departments spent on information technology security in 2012. (68 pages)
Administration Strategy for Mitigating the Theft of U.S. Trade Secrets	Executive Office of the President	February 20, 2013	From the report, "First, we will increase our diplomatic engagement.... Second, we will support industry-led efforts to develop best practices to protect trade secrets and encourage companies to share with each other best practices that can mitigate the risk of trade secret theft.... Third, DOJ will continue to make the investigation and prosecution of trade secret theft by foreign competitors and foreign governments a top priority.... Fourth, President Obama recently signed two pieces of legislation that will improve enforcement against trade secret theft.... Lastly, we will increase public awareness of the threats and risks to the U.S. economy posed by trade secret theft." (141 pages)
National Strategy for Information Sharing and Safeguarding	White House	December 2012	Provides guidance for effective development, integration, and implementation of policies, processes, standards, and technologies to promote secure and responsible information sharing. (24 pages)
Collaborative and Cross-Cutting Approaches to Cybersecurity	White House	August 1, 2012	Michael Daniel, White House cybersecurity coordinator, highlights initiatives in which voluntary, cooperative actions helped to improve the nation's overall cybersecurity.
Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program	Executive Office of the President	December 2011	As a research and development strategy, this plan defines four strategic thrusts: (1) inducing change, (2) developing scientific foundations, (3) maximizing research impact, and (4) accelerating transition to practice. (36 pages)
FY2012 Reporting Instructions for the			Rather than enforcing a static, three-year reauthorization

Federal Information Security Management Act and Agency Privacy Management	OMB	September 14, 2011	process, agencies conduct ongoing authorizations of information systems by implementing continuous monitoring programs. These programs thus fulfill the three-year security reauthorization requirement, so a separate reauthorization process is not necessary. (29 pages)
Cybersecurity Legislative Proposal (Fact Sheet)	White House	May 12, 2011	The Administration's proposal ensures the protection of individuals' privacy and civil liberties through a framework designed expressly to address the challenges of cybersecurity. The Administration's legislative proposal includes management, personnel, intrusion-prevention systems, and data centers.
International Strategy for Cyberspace	White House	May 2011	The strategy marks the first time any Administration has attempted to set forth in one document the U.S. government's vision for cyberspace, including goals for defense, diplomacy, and international development. (30 pages)
National Strategy for Trusted Identities in Cyberspace (NSTIC)	White House	April 15, 2011	The NSTIC aims to make online transactions more trustworthy, thereby giving businesses and consumers more confidence in conducting business online. (52 pages)
Federal Cloud Computing Strategy	White House	February 13, 2011	The strategy outlines how the federal government can accelerate the safe, secure adoption of cloud computing, and provides agencies with a framework for migrating to the cloud. It also examines how agencies can address challenges related to the adoption of cloud computing, such as privacy, procurement, standards, and governance. (43 pages)
25 Point Implementation Plan to Reform Federal Information Technology Management	White House	December 9, 2010	The plan aims to reduce the number of federally run data centers from 2,100 to approximately 1,300, rectify or cancel one-third of troubled IT projects, and require federal agencies to adopt a "cloud first" strategy in which they will move at least one system to a hosted environment within a year. (40 pages)
Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed	Government Accountability Office (GAO)	October 6, 2010	Of the 24 recommendations in the President's May 2009 cyber policy review report, 2 were fully implemented and 22 were partially implemented. Although these efforts appeared to be steps forward, agencies were largely not able to provide milestones and plans that showed when and how implementation of the recommendations was to occur. (66 pages)
			The CNCI establishes a multipronged approach the

Comprehensive National Cybersecurity Initiative (CNCI)	White House	March 2, 2010	federal government is to take in identifying current and emerging cyber threats, shoring up current and future telecommunications and cyber vulnerabilities, and responding to or proactively addressing entities that wish to steal or manipulate protected data on secure federal systems. (5 pages)
Cyberspace Policy Review: Assuring a Trusted and Resilient Communications Infrastructure	White House	May 29, 2009	The President directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. The review team of government cybersecurity experts engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, state governments, international partners, and the legislative and executive branches. The paper summarizes the review team's conclusions and outlines the beginning of the way forward toward a reliable, resilient, trustworthy digital infrastructure for the future. (76 pages)

Source: Highlights compiled by CRS from the White House reports.

Notes: Page counts are documents; other cited resources are web pages. For a list of White House executive orders, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by [author name scrubbed].

Table 6. Cybersecurity Framework (NIST) and Information Sharing

(NIST's Feb. 12, 2014 Cybersecurity Framework, and proposals for cyberthreat information sharing among federal and private stakeholders)

Title	Source	Date	Notes
Information Sharing and Analysis Organizations (ISAOs)	DHS	Continuously updated	Many companies have found it challenging to develop effective information sharing organizationsâ€”or Information Sharing and Analysis Organizations (ISAOs). In response, President Obama issued the 2015 Executive Order 13691 directing DHS to encourage the development of ISAOs.
ISAO Voluntary Guidelines	ISAO Standards Organization	September 2016	The ISAO SO has published initial voluntary guidelines for emerging and established ISAOs. These publications have been developed in response to presidential Executive Order 13691 to provide guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.
The NIST Cybersecurity	Federal Trade	August 31,	From the perspective of the staff of the FTC, NIST's Cybersecurity Framework is consistent with the process-based approach that the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency's educational messages to companies.... The framework and the FTC's approach are fully consistent: The types of things the framework calls for organizations to evaluate are the types of things the

[Framework and the FTC]	Commission	2016	FTC has been evaluating for years in its Section 5 enforcement to determine whether a company's data security and its processes are reasonable. By identifying different risk management practices and defining different levels of implementation, the NIST framework takes a similar approach to the FTC's long-standing Section 5 enforcement.
[Network of 'Things']	NIST	July 28, 2016	The publication provides a basic model aimed at helping researchers better understand the Internet of Things (IoT) and its security challenges. The Network of Things (NoT) model is based on four fundamentals at the heart of IoTâ€"sensing, computing, communication and actuation. The model's five building blocks, called "primitives," are core components of distributed systems. They provide a vocabulary to compare different NoTs that can be used to aid understanding of IoTs. (Note: This document was initially released as a draft back in mid-February 2016, it was under a different technical publication series called NIST Interagency Report (NISTIR) as Draft NISTIR 8063, Internet of Things. After considerable review, it was decided that when the draft becomes approved as final, it will be placed into the Special Publication 800-series - SP 800-183, Network of 'Things'. So this final Special Publication replaces the draft NISTIR 8063). (30 pagesO
[Revision of OMB Circular No. A-130, "Managing Information as a Strategic Resource"]	OMB	July 28, 2016	OMB has revised Circular A-130, "Managing Information as a Strategic Resource," to reflect changes in law and advances in technology. The circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the federal information life cycle. When implemented by agencies, these revisions to the circular will promote innovation, enable appropriate information sharing, and foster the wide-scale and rapid adoption of new technologies while strengthening protections for security and privacy.
[Cybersecurity Framework Feedback: What We Heard and Next Steps]	NIST	June 9, 2016	NIST is developing a minor update of its Cybersecurity Framework based on feedback from its users. A draft of the update will be published for comment in early 2017. The rich body of stakeholder feedback called for other actions that NIST will undertake: Publish a governance process that outlines the process of framework maintenance and evolution and defines the role of stakeholders and how they will continue to work together in the future; Remain as convener of framework stakeholders; and Continue framework outreach and focus on international, small and medium-sized businesses and regulators. (10 pages)
			"This Notice announces a request for public comment on draft products produced by the Information Sharing and

Information Sharing and Analysis Organization	DHS	May 11, 2016	Analysis Organization (ISAO) Standards Organization (SO) in partnership with the six established ISAO SO Standards Working Groups (SWG). This is the first iteration of draft products that will be used in the development of voluntary standards for Information Sharing and Analysis Organizations (ISAOs) as they relate to E.O. 13691." (2 pages)
NPPD Seeks Comments on Cyber Incident Data Repository White Papers	DHS National Protection and Programs Directorate (NPPD)	March 28, 2016	NPPD is seeking public comment on three white papers prepared by NPPD staff. Links to the white papers are posted on the cybersecurity insurance section of DHS.gov: Comments will assist NPPD to further refine the content of the white papers to address the critical need for information sharing as a means to create a more robust cybersecurity insurance marketplace and improve enterprise cyber hygiene practices across the public and private sectors. (2 pages)
Multistakeholder Process To Promote Collaboration on Vulnerability Research Disclosure	NTIA	March 28, 2016	NTIA convened a meeting of a multistakeholder process concerning the collaboration between security researchers and software and system developers and owners to address security vulnerability disclosure. Stakeholders engaged in an open, transparent, consensus-driven process to develop voluntary principles guiding the collaboration between vendors and researchers about vulnerability information. (1 page)
Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents-Notice of Availability	NPPD	February 18, 2016	DHS announced the availability of Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents jointly issued with the Department of Justice (DOJ) in compliance with the act (CISA), which authorizes the voluntary sharing and receiving of cyber threat indicators and defensive measures for cybersecurity purposes, consistent with certain protections, including privacy and civil liberty protections. The CISA guidance documents may be found on http://www.us-cert.gov/ais. (1 page)
NIST Seeking Comments on the Framework for Improving Critical Infrastructure Cybersecurity	National Institute of Standards and Technology (NIST)	December 11, 2015	NIST requested information about the variety of ways in which the Framework for Improving Critical Infrastructure is being used to improve cybersecurity risk management, how best practices using the framework are shared, the relative value of different parts of the framework, the possible need for a framework update, and options for long-term governance of the Framework. (3 pages)
Notice of Public Meeting Regarding Standards for Information Sharing and Analysis Organizations	DHS	October 26, 2015	In accordance with EO 13691, DHS has entered into a cooperative agreement with a non-governmental ISAO Standards Organization led by the University of Texas at San Antonio with support from the Logistics Management Institute (LMI) and the Retail Cyber Intelligence Sharing Center (R-CISC). The notice announces the ISAO Standards Organization's initial public meeting on November 9, 2015, to discuss Standards for the

			development of ISAOs. (2 pages)
Standards for Information Sharing and Analysis Organizations (ISAO)	DHS	May 26, 2015	DHS posted a cooperative agreement funding notice for the outfit that will set standards for ISAO. The grant will be worth up to $11 million over five years. The notice rules out Mitre as a possible bidder, because it excludes federally funded research and development centers and laboratories. However, FFRDCs can be hired by the standards organization for specific projects.
Cybersecurity Risk Management and Best Practices (WG4): Cybersecurity Framework for the Communications Sector	Federal Communications Commission (FCC)	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. (418 pages)
Update on the Cybersecurity Framework	NIST	December 5, 2014	In a status update, NIST said there was widespread agreement among stakeholders that it was too early to update the framework. NIST will consider producing additional guidance for using the framework, including how to apply the little-understood four-tiered system for gauging organizational cybersecurity program sophistication. In general, information and training materials that advance framework use, including illustrative examples, was to be an immediate priority for NIST. (8 pages)
Energy Sector Cybersecurity Framework Implementation Guidance - Draft For Public Comment and Comment Submission Form	Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability	September 12, 2014	Energy companies need not choose 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 instructs users to assess cybersecurity control implementation across 10 domains of cybersecurity practices, such as situational awareness, according to the users' specific "maturity indicator level."
Guidelines for Smart Grid Cybersecurity, Smart Grid Cybersecurity Strategy,	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 stakeholdersâ€”from utilities to providers of energy management services to manufacturers of electric vehicles and charging stationsâ€”can use the methods and supporting information in the report as guidance for assessing risk and identifying and applying

Architecture, and High-Level Requirements			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)
How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts	RAND Corporation	June 2014	Given resource constraints, there are concerns about the effectiveness of information-sharing and fusion activities and, therefore, their value relative to the public funds invested in them. Solid methods for evaluating these efforts are lacking, however, limiting the ability to make informed policy decisions. Drawing on a substantial literature review and synthesis, the report lays out the challenges of evaluating information-sharing efforts that frequently seek to achieve multiple goals simultaneously; reviews past evaluations of information-sharing programs; and lays out a path to improving the evaluation of such efforts. (33 pages)
Sharing Cyberthreat Information Under 18 USC Â§ 2702(a)(3)	Department of Justice (DOJ)	May 9, 2014	DOJ issued guidance for Internet service providers to assuage legal concerns about information sharing. The white paper interprets the Stored Communications Act, which prohibits providers from voluntarily disclosing customer information to governmental entities. The paper says that the law does not prohibit companies from divulging data in the aggregate, without any specific details about identifiable customers. (7 pages)
Antitrust Policy Statement on Sharing of Cybersecurity Information	DOJ and Federal Trade Commission (FTC)	April 10, 2014	Information-sharing about cyber threats can be done lawfully as long as companies are not discussing competitive information such as pricing, the Justice Department and Federal Trade Commission said in a joint statement. "Companies have told us that concerns about antitrust liability have been a barrier to being able to openly share cyber threat information," said Deputy Attorney General James Cole. "Antitrust concerns should not get in the way of sharing cybersecurity information." (9 pages)
Framework for Improving Critical Infrastructure Cybersecurity	NIST	February 12, 2014	The voluntary framework consists of cybersecurity standards that can be customized to various sectors and adapted by both large and small organizations. DHS announced the Critical Infrastructure Cyber Community (C^3)â€”or "C-cubed"â€”voluntary program. The C^3 program gives state and local governments and companies that provide critical services, such as cell phones, email, banking, and energy, direct access to DHS cybersecurity experts 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)

Update on the Development of the Cybersecurity Framework	NIST	January 15, 2014	From the document, "While stakeholders have said they see the value of guidance relating to privacy, many comments stated a concern that the methodology did not reflect consensus private sector practices and therefore might limit use of the Framework. Many commenters also stated their belief that privacy considerations should be fully integrated into the Framework Core." (3 pages)
Cybersecurity Framework	NIST	October 22, 2013	NIST sought comments on the preliminary version of the Cybersecurity Framework. Executive Order 13636 directed NIST to work with stakeholders to develop such a framework to reduce cyber risks to critical infrastructure. (47 pages)
Discussion Draft of the Preliminary Cybersecurity Framework	NIST	August 28, 2013	The framework provides a common language and mechanism for organizations to (1) describe current cybersecurity posture; (2) describe their target state for cybersecurity; (3) identify and prioritize opportunities for improvement within the context of risk management; (4) assess progress toward the target state; and (5) foster communications among internal and external stakeholders. (36 pages)
Cyber Security Task Force: Public-Private Information Sharing	Bipartisan Policy Center	July 2012	Outlines a series of proposals to enhance information sharing. The recommendations have two major components: (1) mitigating perceived legal impediments to information sharing, and (2) incentivizing private-sector information sharing by alleviating statutory and regulatory obstacles. (24 pages)
Annual Report to Congress 2012: National Security Through Responsible Information Sharing	Information Sharing Environment	June 30, 2012	The report states, "This Report, which PM-ISE is submitting on behalf of the President, incorporates input from our mission partners and uses their initiatives and PM-ISE's management activities to provide a cohesive narrative on the state and progress of terrorism-related responsible information sharing, including its impact on our collective ability to secure the nation and our national interests." (188 pages)
NICE Cybersecurity Workforce Framework	National Initiative for Cybersecurity Education (NICE)	November 21, 2011	The federal government's adoption and implementation of cloud computing depend upon a variety of technical and nontechnical factors. A fundamental reference point, based on the NIST definition of cloud computing, is needed to describe an overall framework that can be used government-wide. The document presents the NIST Cloud Computing Reference Architecture and Taxonomy that will accurately communicate the components and offerings of cloud computing. (35 pages)
Improving our Nation's Cybersecurity through the Public-Private	Business Software Alliance, Center for Democracy and Technology, U.S. Chamber of	March 8, 2011	The paper proposes expanding the existing partnership within the framework of the National Infrastructure Protection Plan. Specifically, it makes a series of recommendations that build upon the conclusions of

Partnership: A White Paper	Commerce, Internet Security Alliance, and Tech America		President Obama's *Cyberspace Policy Review*. (26 pages)
Efforts to Improve Information Sharing Need to Be Strengthened	Government Accountability Office (GAO)	August 27, 2003	Information on threats, methods, and techniques of terrorists is not routinely shared, and the information that is shared is not perceived as timely, accurate, or relevant. (59 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are web pages.

Table 7. Department of Homeland Security (DHS)

(reports and audits)

Title	Source	Date	Notes
Office of Cybersecurity and Communications (CS&C)	DHS	Continuously Updated	• works to prevent or minimize disruptions to critical information infrastructure to protect the public, the economy, and government services and • leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sectorâ€”the ".com" domainâ€”to increase the security of critical networks.
Continuous Diagnostic and Mitigation Program	DHS	Continuously Updated	An initiative to deploy continuous monitoring at U.S. federal government agencies will be done in phases, with the initial rollout occurring over three years. The initial phase is aimed at getting federal civilian agencies to employ continuous diagnostic tools to improve vulnerability management, enforce strong compliance settings, manage hardware and software assets, and establish white-listing of approved services and applications.
Critical Infrastructure Protection: Improvements Needed for DHS's Chemical Facility Whistleblower Report Process	Government Accountability Office (GAO)	July 12, 2016	The Chemical Facility Anti-Terrorism Standards (CFATS) Act of 2014 required DHS to establish a whistleblower process. Employees and contractors at hundreds of thousands of U.S. facilities with hazardous chemicals can play an important role in helping to ensure CFATS compliance by submitting a whistleblower report when they suspect noncompliance This report addresses (1) the number and types of CFATS whistleblower reports DHS received, and any actions DHS took as a result, and (2) the extent to which DHS has implemented and followed a process to address the whistleblower reports, including reports of retaliation against whistleblowers. (49 pages)

Cybersecurity Information Sharing Act of 2015 Final Guidance Documents-Notice of Availability	DHS	June 15, 2016	DHS is announcing the availability of Cybersecurity Information Sharing Act of 2015 (CISA) Final Guidance Documents jointly issued with the Department of Justice (DOJ) in compliance with the act, which authorizes the voluntary sharing and receiving of cyber threat indicators and defensive measures for cybersecurity purposes, consistent with certain protections, including privacy and civil liberty protections. The CISA-mandated final procedures and guidance, as well as an updated version of the non-federal entity sharing guidance, may be found at www.us-cert.gov/ais. (2 pages)
DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System	GAO	January 28, 2016	DHS's National Cybersecurity Protection System (NCPS) is partially meeting its stated system objectivesâ€¦. Federal agencies have adopted NCPS to varying degrees. The 23 agencies required to implement the intrusion detection capabilities had routed some traffic to NCPS intrusion detection sensors. However, only 5 of the 23 agencies were receiving intrusion prevention services, but DHS was working to overcome policy and implementation challenges. Further, agencies have not taken all the technical steps needed to implement the system, such as ensuring that all network traffic is being routed through NCPS sensors. This occurred in part because DHS has not provided network routing guidance to agencies. As a result, DHS has limited assurance regarding the effectiveness of the system. (61 pages)
DHS Can Strengthen Its Cyber Mission Coordination Efforts	Department of Homeland Security (DHS), OIG	September 15, 2015	DHS still struggles to coordinate its cyber-response activities and lacks an automated information-sharing tool to share cyberthreat data among components within the departmentâ€”let alone between government and the private sector, which the Obama Administration and some lawmakers have been pressing for. In addition, the IG found scattershot training for cybersecurity professionals in the department, with some analysts paying for their own training courses to keep their skills fresh. (36 pages)
IT Security Suffers from Noncompliance	DHS Office of Inspector General (OIG)	December 22, 2014	DHS has made progress in improving its information security program, but noncompliance by several DHS component agencies is undermining that effort. The OIG raised concerns over a lack of compliance by these components and urged DHS leadership to strengthen its oversight and enforcement of existing security policies. (2 pages)
Health Insurance Marketplaces Generally Protected Personally Identifiable Information but Could Improve	Department of Homeland Security (DHS), OIG	September 22, 2014	The websites and databases in some state health insurance exchanges are still vulnerable to attack, putting personally identifiable information at risk. The report examined the websites and databases of the federal insurance exchange, as well as the state exchanges for Kentucky and New

Certain Information Security Controls			Mexico.
Implementation Status of the Enhanced Cybersecurity Services Program	DHS OIG	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 the program and 22 companies had signed memorandums of agreement to join the program. Although progress has been made, the 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)
The Critical Infrastructure Cyber Community CÂ³ Voluntary Program	Department of Homeland Security (DHS)	February 12, 2014	The CÂ³ Voluntary Program serves as a point of contact and a customer relationship manager to assist organizations with using the Cybersecurity Framework and guide interested organizations and sectors to DHS and other public and private-sector resources to support use of the framework.
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 eying further improvement of the framework, changes that call for DHS to "de-emphasize the current focus on incentives." Partly, ITI recognizes the cyber order can produce change even in an environment in which fiscal constraints and congressional inaction stall carrots for adoption, but ITI and others "do not want incentives if they come at the cost of "compliance-based programs." (3 pages)
Evaluation of DHS' Information Security Program for Fiscal Year 2013	DHS OIG	November 2013	The report reiterates that the agency uses outdated security controls and Internet connections that are not verified as trustworthy and that the agency does not review its top-secret information systems for vulnerabilities. (50 pages)
DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Center	DHS OIG	October 2013	DHS could do a better job sharing information among the five federal centers that coordinate cybersecurity work. The department's National Cybersecurity and Communications Integration Center (NCCIC) is tasked with sharing information about malicious activities on government networks with cybersecurity offices within DOD, the Federal Bureau of Investigation (FBI), and federal intelligence agencies. But the DHS center and the five federal cybersecurity hubs all have different technology and resources, preventing them from sharing

			intrusions, threats, or awareness information and restricting their ability to coordinate responses. The centers also have not created a standard set of categories for reporting incidents. (29 pages)
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts	GAO	September 17, 2013	Within DHS, o at a key cybersecurity component is vacant, in large part due to steep competition in recruiting and hiring qualified personnel. National Protection and Programs Directorate (NPPD) officials cited challenges in recruiting cyber professionals because of the length of time taken to conduct security checks to grant top-secret security clearances and low pay in comparison with the private sector. (47 pages)
DHS Can Take Actions to Address Its Additional Cybersecurity Responsibilities	DHS	June 2013	The National Protection and Programs Directorate (NPPD) was audited to determine whether the Office of Cybersecurity and Communications had effectively implemented its additional cybersecurity responsibilities to improve the security posture of the federal government. Although it has made some progress, NPPD can make further improvements to address its additional cybersecurity responsibilities. (26 pages)
Privacy Impact Assessment for EINSTEIN 3 Accelerated (E^3A)	DHS	April 19, 2013	DHS deployed EINSTEIN 3 Accelerated (E3A) to enhance cybersecurity analysis, situational awareness, and security response. Under DHS's direction, Internet service providers will administer intrusion prevention and threat-based decisionmaking on network traffic entering and leaving participating federal civilian executive branch agency networks. This Privacy Impact Assessment (PIA) was being conducted because E3A will include analysis of federal network traffic, which may contain personally identifiable information. (27 pages)
Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts	GAO	April 11, 2013	Until DHS and its sector partners develop appropriate outcome-oriented metrics, it will be difficult to gauge the effectiveness of efforts to protect the nation's core and access communications networks and the Internet's critical support components from cyber incidents. Although no cyber incidents affecting the nation's core and access networks have been reported, communications networks operators can use reporting mechanisms established by the Federal Communications Commission and DHS to share information on outages and incidents. (45 pages)
Federal Support for and Involvement in State and Local Fusion Centers	U.S. Senate Permanent Subcommittee on Investigations	October 3, 2012	A two-year bipartisan investigation found that DHS efforts to engage state and local intelligence "fusion centers" has not yielded significant useful information to support federal counterterrorism intelligence efforts. In Section VI, "Fusion Centers Have Been Unable to Meaningfully Contribute to Federal Counterterrorism Efforts," Part G, "Fusion Centers May Have Hindered, Not Aided, Federal Counterterrorism Efforts," the report discusses the Russian "cyberattack" in Illinois. (141 pages)

CyberSkills Task Force Report	DHS	October 2012	DHS's task force on CyberSkills proposes far-reaching improvements to enable the department to recruit and retain the cybersecurity talent it needs. (41 pages)
DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened	GAO	September 23, 2010	DHS has not developed an effective way to ensure that critical national infrastructure, such as electrical grids and telecommunications networks, can bounce back from a disaster. DHS conducted surveys and vulnerability assessments of critical infrastructure to identify gaps but has not developed a way to measure whether owners and operators of that infrastructure adopt measures to reduce risks. (46 pp)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are web pages.

Table 8. Department of Defense (DOD)

(reports by and audits of)

Title	Source	Date	Notes
Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program	DOD	Continuously Updated	DOD established the Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program to enhance and supplement DIB participants' capabilities to safeguard DOD information that resides on or transits DIB unclassified networks or information systems. The public-private cybersecurity partnership is designed to improve DIB network defenses, reduce damage to critical programs, and increase DOD and DIB cyber situational awareness. Under the DIB CS/IA Program, DOD and DIB participants share unclassified and classified cyber threat information.
Program Protection and System Security Engineering Initiative	DOD Systems Engineering	Continuously Updated	DOD systems have become increasingly networked, software-intensive, and dependent on a complicated global supply chain, which has increased the importance of security as a systems engineering design consideration. In response to this new reality, DOD has established Program Protection/System Security Engineering as a key discipline to protect technology, components, and information from compromise through the cost-effective application of countermeasures to mitigate risks posed by threats and vulnerabilities. The analysis, decisions, and plans of acquisition programs are documented in a Program Protection Plan, which is updated prior to every milestone decision.
			This final rule responds to public comments and

DOD's Defense Industrial Base Cybersecurity Activities	DOD	October 4, 2016	updates DOD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities. This rule implements mandatory cyber incident reporting requirements for DOD contractors and subcontractors who have agreements with DOD. In addition, the rule modifies eligibility criteria to permit greater participation in the voluntary DIB CS information sharing program. (6 pages)
What is NORAD's Role in Military Cyber Attack Warning?	Homeland Security Affairs	May 2016	The essay traces NORAD's warning mission history, discusses the basic concepts involved with cyberattacks, identifies key U.S. and Canadian military cyber organizations, and examines significant U.S. and Canadian cyberspace government policies. It then proposes three potential new courses of action for NORAD, identifying advantages, disadvantages, and proposed solutions to implementation. (24 pages)
DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents, Report to Congressional Committees	*GAO*	April 4, 2016	This report assesses the extent to which DOD has developed guidance that clearly defines the roles and responsibilities for providing support to civil authorities in response to a cyber incident. GAO reviewed DOD DSCA guidance, policies, and plans; and met with relevant DOD, National Guard Bureau, and Department of Homeland Security officials. (31 pages)
Department of Defense Provides Government Contractors Grace Period for Compliance with Key Cybersecurity Requirements	*National Law Review*	January 4, 2016	The Pentagon is giving military contractors an 18-month extension to comply with certain cybersecurity requirements in the Defense Federal Acquisition Regulation Supplement (DFARS). The decision to allow contractors a grace period was made following public comments in December 2015.
National Guard Set to Activate Additional Cyber Units	U.S. Army	December 9, 2015	The National Guard announced plans to activate 13 additional cyber units spread throughout 23 states by the end of FY2019. Seven new Army Guard cyber protection teams, or CPTs, will be activated across Alabama, Arkansas, Colorado, Illinois, Kentucky, Louisiana, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New York, North Dakota, South Dakota, Tennessee, Texas, Utah, and Wisconsin. They join four previously announced Army Guard CPTs spread across California, Georgia, Indiana, Maryland, Michigan, and Ohio.
Department of			DOD is revising its DoD-DIB Cybersecurity (CS) Activities regulation to mandate reporting of cyber

Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities	DOD Chief Information Officer	October 2, 2015	incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support, and modify eligibility criteria to permit greater participation in the voluntary DoD- DIB CS information sharing program. (8 pages)
Cyber Security DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2014, Through July 31, 2015	DOD Office of Inspector General (OIG)	September 25, 2015	In the span of one year, the Pentagon addressed fewer than half of the recommendations to shore up cyber vulnerabilities identified by its OIG. The Defense Department addressed 93 of 229 cyber recommendations made by the OIG between August 1, 2014 and July 31, 2015, according to a summary of a new audit released by the IG's office. DOD left the majority of recommendationsâ€”136â€”unresolved.
Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services	DOD	August 26, 2015	DOD is issuing an interim rule amending DFARS to implement a section of the National Defense Authorization Act for Fiscal Year 2013 and a section of the National Defense Authorization Act for Fiscal Year 2015, both of which require contractor reporting on network penetrations. Additionally, this rule implements DOD's policy on the purchase of cloud computing services. (10 pages)
Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems	Government Accountability Office (GAO)	June 2, 2015	DOD components have identified technical and policy changes to help protect classified information and systems from future insider threats, but DOD is not consistently collecting this information to support management and oversight responsibilities. DOD has not identified a program office to oversee the insider-threat program. Without an office dedicated to oversight of insider-threat programs, DOD may not be able to ensure the collection of all needed information and could face challenges in establishing goals and in recommending resources and improvements to address insider threats. This is an unclassified version of a classified report GAO issued in April 2015. (55 pages)
The DOD Cyber Strategy	DOD	April 17, 2015	Deterrence is a key part of the new cyber strategy, which describes the department's contributions to a broader national set of capabilities to deter adversaries from conducting cyberattacks. The strategy sets five strategic goals and establishes specific objectives for DOD to achieve over the next five years and beyond. (42 pages)
Cyber Insurance: Managing Cyber Risk	Institute for Defense Analyses	April 2015	The paper provides an overview of the components of cyber insurance, discusses the role of the government, and examines specific implications to the Defense

			Department. (14 pages)
Excepted Service (DOD)	Office of Personnel Management (OPM)	March 5, 2015	DOD is given authority to make permanent, time-limited, and temporary appointments not to exceed 3,000 positions that require unique cybersecurity skills and knowledge to perform cyber risk and strategic analysis, incident handling and malware/vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, investigative analysis, and cyber-related infrastructure inter-dependency analysis. (3 pages)
DOT&E FY 2014 Annual Report	DOD Office of the Director, Operational Test and Evaluation (OT&E)	January 2015	A series of live fire tests of the military's computer networks security in 2015 found many combatant commands could be compromised by low-to-middling-skilled hackers and might not be able to "fight through" in the face of enemy cyberattacks. The assessment echoes previous OT&E annual assessments, which routinely found that military services and combatant commands did not have a sufficiently robust security posture or training to repel sustained cyberattacks during battle. (91 pages)
A Review of the U.S. Navy Cyber Defense Capabilities: Abbreviated Version of a Classified Report	National Research Council (NRC)	January 2015	The NRC appointed an expert committee to review the U.S. Navy's cyber defense capabilities. The Department of the Navy determined that the committee's final report is classified in its entirety under Executive Order 13526 and therefore cannot be made available to the public. A Review of U.S. Navy Cyber Defense Capabilities, the abbreviated report, provides background information on the full report and the committee that prepared it. (13 pages)
Training Cyber Warriors: What Can Be Learned from Defense Language Training?	RAND Corporation	January 20015	The study examines what the military services and national security agencies have done to train linguist personnel with skills in critical languages other than English and the kinds of language training provided to build and maintain this segment of the workforce. The study draws from published documents, research literature, and interviews of experts in both language and cyber. (97 pages)
DOD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process	DOD OIG	December 4, 2014	Report states that the DOD chief information officer "did not develop an implementation plan that assigned roles and responsibilities as well as associated tasks, resources and milestones," despite promises that an implementation plan would directly follow the cloud strategy's release. (40 pages)
			The results of this analysis reflect DOD's current view of its requirements for successful conduct of

Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense	National Guard	August 21, 2014	cyberspace operations, leveraging a Total Force solution. DOD assesses there can be advantages to using reserve component (RC) resources for Cyber Mission Force (CMF) missions, such as providing load sharing with active duty forces, providing available surge capacity if authorized to activate, and maintaining DOD-trained forces to defend national critical infrastructure. (45 pages)
State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation and Appendix E: State-of-the-Art Resources (SOAR) Matrix (Excel spreadsheet)	Institute for Defense Analyses Report P-5061	July 2014	The paper assists DOD program managers and their staffs in making effective software assurance and software supply chain risk management decisions. It describes some key gaps identified in the course of the study, including difficulties in finding unknown malicious code, obtaining quantitative data, analyzing binaries without debug symbols, and obtaining assurance of development tools. Additional challenges were found in the mobile environment. (234 pages)
Military and Security Developments Involving the People's Republic of China 2013 (Annual Report to Congress)	DOD	May 6, 2013	China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense-industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high-technology industries, policy-maker interest in U.S. leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis. (92 pages)
FY2012 Annual Report	DOD	January 2013	The annual report to Congress by J. Michael Gilmore, director of Operational Test and Evaluation, assesses the operational effectiveness of systems being developed for combat. See Information Assurance (I/A) and Interoperability (IOP) chapter, pages 305-312, for information on network exploitation and compromise exercises. (372 pages)
Resilient Military Systems and the Advanced Cyber Threat	Department of Defense (DOD) Science Board	January 2013	The report states that, despite numerous Pentagon actions to parry sophisticated attacks by other countries, efforts are "fragmented" and DOD "is not prepared to defend against this threat." The report lays out a scenario in which cyberattacks in conjunction with conventional warfare damaged the ability of U.S. forces to respond, creating confusion on the battlefield

			and weakening traditional defenses. (146 pages)
Crisis and Escalation in Cyberspace	RAND Corporation	December 2012	The report considers how the Air Force should integrate kinetic and nonkinetic operations. Central to this process was careful consideration of how escalation options and risks should be treated, which, in turn, demanded a broader consideration across the entire crisis-management spectrum. Such crises can be managed by taking steps to reduce the incentives for other states to step into crisis, controlling the narrative, understanding the stability parameters of the crises, and trying to manage escalation if conflicts arise from crises. (200 pages)
Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight	GAO	July 9, 2012	DOD's oversight of electronic warfare capabilities may be further complicated by its evolving relationship with computer network operations, which is also an information operations-related capability. Without clearly defined roles and responsibilities and updated guidance regarding oversight responsibilities, DOD does not have reasonable assurance that its management structures will provide effective department-wide leadership for electronic warfare activities and capabilities development and ensure effective and efficient use of its resources. (46 pages)
Cloud Computing Strategy	DOD, Chief Information Officer	July 2012	The DOD Cloud Computing Strategy introduces an approach to move the department from the current state of a duplicative, cumbersome, and costly set of application silos to an end state, which is an agile, secure, and cost-effective service environment that can rapidly respond to changing mission needs. (44 pages)
DOD Information Security Program: Overview, Classification, and Declassification	DOD	February 24, 2012	Describes the DOD Information Security Program and provides guidance for classification and declassification of DOD information that requires protection in the interest of national security. (84 pages)
Cyber Sentries: Preparing Defenders to Win in a Contested Domain	Air War College	February 7, 2012	The paper examines the current impediments to effective cybersecurity workforce preparation and offers new concepts to create "Cyber Sentries" through realistic training, network authorities tied to certification, and ethical training. These actions present an opportunity to significantly enhance workforce quality and allow DOD to operate effectively in the contested cyber domain in accordance with the vision established in its Strategy for Cyberspace Operations. (38 pages)
Anomaly	Defense Advanced		The report describes a system for preventing leaks by

Detection at Multiple Scales (ADAMS)	Research Projects Agency (DARPA)	November 9, 2011	seeding believable disinformation in military information systems to help identify individuals attempting to access and disseminate classified information. (74 pages)
Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates	GAO	July 29, 2011	The letter discusses DOD's cyber and information assurance budget for FY2012 and future years' defense spending. The review's objectives were to (1) assess the extent to which DOD has prepared an overarching budget estimate for full-spectrum cyberspace operations across the department and (2) identify the challenges DOD has faced in providing such estimates. (33 pages)
Legal Reviews of Weapons and Cyber Capabilities	Secretary of the Air Force	July 27, 2011	Report concludes the Air Force must subject cyber capabilities to legal review for compliance with the Law of Armed Conflict and other international and domestic laws. The Air Force judge advocate general must ensure that all cyber capabilities "being developed, bought, built, modified, or otherwise acquired by the Air Force" undergo legal reviewâ €”except for cyber capabilities within a Special Access Program, which must undergo review by the Air Force general counsel. (7 pages)
Department of Defense Strategy for Operating in Cyberspace	DOD	July 2011	An unclassified summary of DOD's cybersecurity strategy. (19 pages)
Defending a New Domain	*Foreign Affairs*	September/October 2010	In 2008, DOD suffered a significant compromise of its classified military computer networks when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The previously classified incident was the most significant breach of U.S. military computers ever and served as an important wake-up call.
Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems	GAO	September 15, 2010	OMB and NIST established policies and guidance for civilian non-national security systems, and other organizations, including the Committee on National Security Systems (CNSS), DOD, and the U.S. intelligence community, have developed policies and guidance for national security systems. GAO assessed the progress of federal efforts to harmonize policies and guidance for these two types of systems. (38 pages)
Computer			Defense Information Systems Agency (DISA) estimates indicate that DOD may have been attacked

Attacks at Department of Defense Pose Increasing Risk	GAO	May 1996	as many as 250,000 times in 1995. However, the exact number is not known because, according to DISA, only about 1 in 150 attacks is actually detected and reported. In addition, in testing its systems, DISA attacks and successfully penetrates DOD systems 65% of the time. (48 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are web pages.

Table 9. National Institute of Standards and Technology (NIST)

(includes selected NIST standards, guidance, Special Publications (SP), and grants)

Title	Date	Notes
Computer Security Division, Computer Security Resource Center	Continuously Updated	Compilation of laws, regulations, and directives from 2000 to 2007 that govern the creation and implementation of federal information security practices. These laws and regulations provide an infrastructure for overseeing implementation of required practices and charge NIST with developing and issuing standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.
NIST Announces the release of 3 DRAFT NISTIRs (NIST Internal Reports)	October 4, 2016	(1) Draft NISTIR 8151, Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy; (2) Draft NISTIR 8149, Developing Trust Frameworks to Support Identity Federations; and, (3) Draft NISTIR 8138, Vulnerability Description Ontology (VDO): a Framework for Characterizing Vulnerabilities.
Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue	September 2016	NIST's "mobile threat catalogue" sketches out parts of a mobile device strategy that need special attention, including securing physical access to smartphones and tablets, as well as authenticating who is using the device with passwords, fingerprints or voice recognition. "[M]obile device components are under constant development and are sourced from tens of thousands of original equipment manufacturers." Firmware could contain its own vulnerabilities, and "can increase the overall attack surface of the mobile device." (50 pages)
Cybersecurity Risk Assessment Tool (Baldrige Cybersecurity Excellence Builder)	September 2016	The Baldrige Cybersecurity Excellence Builder is intended to help organizations ensure that their cybersecurity systems and processes support the enterprises' larger organizational activities and functions. The tool "is not a one-size-fits-all approach. It is adaptable and scalable to your organization's needs, goals, capabilities, and environment. It does not prescribe how you should structure your organization's cybersecurity policies and operations. Through interrelated sets of open-ended questions, it encourages you to use the approaches that best fit your organization." (35 pages)
DRAFT NIST		

Special Publication 800-63B Digital Authentication Guideline	August 3, 2016	In an update to its Digital Authentication Guidelines, NIST calls for phasing out two-factor authentication via SMS messaging, saying that the method does not offer adequate security. The guidance applies to government service providers.
Network of 'Things'	July 28, 2016	The publication provides a basic model aimed at helping researchers better understand the Internet of Things (IoT) and its security challenges. The Network of Things (NoT) model is based on four fundamentals at the heart of IoTâ€" sensing, computing, communication and actuation. The model's five building blocks, called *primitives*, are core components of distributed systems. They provide a vocabulary to compare different NoTs that can be used to aid understanding of IoTs. (30 pages)
NIST 'RAMPS' Up Cybersecurity Education and Workforce Development With New Grants	May 12, 2016	NIST is offering up to $1 million in grants to establish up to eight Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development. Applicants must be nonprofit organizations, including institutions of higher education, located in the United States or its territories. Applicants must also demonstrate through letters of interest that at least one of each of the following types of organizations is interested in being part of the proposed regional alliance: K-12 school or Local Education Agency (LEA), institution of higher education or college/university system, and a local employer.
NIST seeking comments on the Framework for Improving Critical Infrastructure Cybersecurity	December 11, 2015	In this Request for Information (RFI), NIST requests information about the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance of the Framework. (3 pages)
Pilot Projects to Improve Cybersecurity, Reduce Online Theft	September 21, 2015	NIST is awarding $3.7 million to support three pilot programs that aim to make online transactions for health care, government services, transportation, and the Internet of Things (IoT) more secure and private. This is the fourth round of grants given to support the NSTIC effort, which was launched in 2011 by the Obama Administration to encourage secure, efficient, easy-to-use, and interoperable identity credentials for online use.
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (SP 800-171)	June 2015	SP 800-171 is a final draft of security controls for federal contractors to follow when handling a class of data known as "controlled unclassified information." The document will become a formal requirement for government contractors in 2016 through an anticipated update to federal acquisition regulations. Controlled unclassified information is an umbrella term for a wide range of data that includes personally identifiable information, financial transactions, and geospatial images. (76 pages)
Assessing Security and Privacy Controls in Federal Information Systems and	December	The publication provides organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate, which will contribute to systems that are more resilient in the face of cyberattacks and other threats. This "Build It Right" strategy is coupled with a variety

Organizations: Building Effective Assessment Plans (SP 800-53A, rev. 4)	12, 2014	of security controls for continuous monitoring to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions. (487 pages)
NIST/NCCoE Establishment of a Federally Funded Research and Development Center	September 22, 2014	The MITRE Corporation was awarded NIST's cybersecurity Federally Funded Research and Development Center (FFRDC) contract worth up to $5 billion over five years. MITRE already operates six individual FFRDCs for agencies including the DOD and the Federal Aviation Administration (FAA). It is also active in cybersecurity, managing the Common Vulnerabilities and Exposures database, which catalogues software security flaws. In addition, it developed specifications for the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) under DHS contract.
Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems	May 13, 2014	NIST launched a four-stage process to develop detailed guidelines for "systems security engineering," adapting a set of widely used international standards for systems and software engineering to the specific needs of security engineering. The agency released the first set of those guidelines for public comment in a draft document. (121 pages)
Memorandum of Understanding (MOU)	December 2, 2010	The MOU, signed by NIST, DHS, and the Financial Services Sector Coordinating Council, formalized the parties' intent to expedite the coordinated development and availability of collaborative research, development, and testing activities for cybersecurity technologies and processes based upon the financial services sector's needs. (4 pages)

Source: Highlights compiled by CRS from the reports.

Note: Page counts are documents; other cited resources are web pages.

Author Contact Information

[author name scrubbed], Senior Research Librarian ([email address scrubbed], [phone number scrubbed])