CRS Reports & Analysis

Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources
November 14, 2017 (R44408)
Jump to Main Text of Report
Rita Tehan, Information Research Specialist (rtehan@crs.loc.gov, 7-6739)

Related Author

- Rita Tehan

Contents

Tables

Summary

As online attacks grow in volume and sophistication, the United States is expanding its cybersecurity efforts. Cybercriminals continue to develop new ways to ensnare victims, whereas nation-state hackers compromise companies, government agencies, and businesses to create espionage networks and steal information. Threats come from both criminals and hostile countries, especially China, Russia, Iran, and North Korea.

Much is written on this topic, 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:

- **Table 1**—cybercrime, data breaches and security, including hacking, real-time attack maps, and statistics (such as economic estimates)
- **Table 2**—national security, cyber espionage, and cyberwar, including Stuxnet, China, and the Dark Web
- **Table 3**—cloud computing, the Internet of Things (IoT), smart cites, and FedRAMP

The following reports comprise a series of authoritative reports and resources on these additional cybersecurity topics:

- CRS Report R44405, *Cybersecurity: Overview Reports and Links to Government, News, and Related Resources*, by Rita Tehan.
- CRS Report R44406, *Cybersecurity: Education, Training, and R&D Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44408, *Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44410, *Cybersecurity: Critical Infrastructure Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44417, *Cybersecurity: State, Local, and International Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R44427, *Cybersecurity: Federal Government Authoritative Reports and Resources*, by Rita Tehan.
- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.
- CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan.

Introduction

As online attacks grow in volume and sophistication, the United States is expanding its cybersecurity efforts. Cybercriminals continue to develop new ways to ensnare victims, whereas nation-state hackers compromise companies, government agencies, and businesses to create espionage networks and steal information. Threats come from both criminals and hostile countries, especially China, Russia, Iran, and North Korea.

Much is written on this topic, 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:

- **Table 1**—cybercrime, data breaches and security, including hacking, real-time attack maps, and statistics (such as economic estimates)
- **Table 2**—national security, cyber espionage, and cyberwar, including Stuxnet, China, and the Dark Web
- **Table 3**—cloud computing, the Internet of Things (IoT), and FedRAMP

Table 1. Cybercrime, Data Breaches, and Data Security

(include data breaches[1], hacking, real-time attack maps, statistics)

Title	Source	Date	Notes
The Cyberfeed	Anubis Networks	Continuously Updated	This site provides real-time threat intelligence data worldwide.
Digital Attack Map	Arbor Networks	Continuously Updated	The map is powered by data fed from 270+ ISP customers worldwide who have agreed to share network traffic and attack statistics. The map displays global activity levels in observed attack traffic, which it collected anonymously, and does not include any identifying information about the attackers or victims involved in any particular attack.
Cyber Incident Timeline	Center for Strategic & International Studies (CSIS)	Continuously Updated	The CSIS's Strategic Technologies program's interactive "Cyber Incident Timeline" details the successful attacks on government agencies, defense and high tech companies, and international economic crimes with losses of more than $1 million, since 2006. It includes news reports and videos on most incidents.
Summary of U.S. State Data Breach Notification Statutes	Davis Wright Tremaine LLP	Continuously Updated	Click on any of the states to see a full summary of their data breach notification statute.
DataBreaches.net	Dissent (pseudonym)	Continuously Updated	This site is a combination of news aggregation, investigative reporting, and commentary on data breaches and data breach laws. Can browse data breaches by sector.
ThreatExchange	Facebook	Continuously Updated	ThreatExchange is a set of application programming interfaces, or APIs, that let disparate companies trade information about the latest online attacks. Built atop the Facebook Platform —a repository of a standard set of tools for coding applications within the worldwide social network —ThreatExchange is used by Facebook and a handful of other companies, including Tumblr, Pinterest, Twitter, and Yahoo. Access to the service is strictly controlled, but [Facebook] hopes to include more companies as time goes on.
Federal Trade Commission List of Settled Data Security Cases	Federal Trade Commission (FTC)	Continuously Updated	The FTC's Legal Resources website offers a compilation of laws, cases, reports, and more. The user can filter the FTC's legal documents by type

			(case) and topic (data security), resulting in a list of 55 data security cases from 2000 to 2015, in reverse chronological order. Clicking the case name provides more details, such as the case citation, timeline, press releases, and pertinent legal documents.
Threat Intelligence Database	Fidelis Barncat	Continuously Updated	The database includes more than 100,000 records with configuration settings extracted from malware samples gathered during Fidelis' incident response investigations and other intelligence gathering operations over the past decade. The typical malware sample includes a large number of configuration elements, including those controlling the behavior of the malware on the host and others related to command-and-control traffic. Barncat is updated with hundreds of new configuration records each day. Barncat is available for use by CERTs, research organizations, government entities, ISPs and other large commercial enterprises. Access is free, but users must request access and meet specific criteria.
IdentityTheft.gov	FTC	Continuously Updated	The one-stop website is integrated with the FTC's consumer complaint system, allowing consumers who are victims of identity theft to rapidly file a complaint with the FTC and then get a personalized guide to recovery that helps streamline many of the steps involved. The upgraded site, which is mobile and tablet accessible, offers an array of easy-to-use tools that enables identity theft victims to create the documents they need to alert police, the main credit bureaus, and the Internal Revenue Service (IRS) among others.
HHS Breach Portal: Breaches Affecting 500 or More Individuals	Health and Human Services (HHS)	Continuously Updated	As required by Section 13402(e)(4) of the HITECH Act, P.L. 111-5 HHS must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are posted in a more accessible format that allows users to search and sort the posted breaches. Additionally, the format includes brief summaries of the breach cases that the Office for Civil Rights (OCR) has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information.
Combatting Cyber Crime	Homeland Security	Continuously Updated	DHS works with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.

HoneyMap	Honeynet Project	Continuously Updated	The HoneyMap displays malicious attacks as they happen. Each red dot represents an attack on a computer. Yellow dots represent "honeypots" or systems set up to record incoming attacks. The black box on the bottom gives the location of each attack. The Honeynet Project is an international 501(c)(3) nonprofit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security.
Data Breaches	Identity Theft Resource Center	Continuously Updated	The report presents detailed information about data exposure events along with running totals for a specific year. Breaches are broken down into five categories: business, financial/credit/financial, educational, governmental/military, and medical/healthcare.
Regional Threat Assessment: Infection Rates and Threat Trends by Location	Microsoft Security Intelligence Report (SIR)	Continuously Updated	The report provides data on infection rates, malicious websites, and threat trends by regional location, worldwide. (Note: Select "All Regions" or a specific country or region to view threat assessment reports.)
No More Ransom	National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Center, Kaspersky Lab and Intel Security	Continuously Updated	The online portal offers a one-stop shop for battling ransomware infections.
ThreatWatch	NextGov	Continuously Updated	ThreatWatch is a snapshot of the data breaches hitting organizations and individuals, globally, on a daily basis. It is not an authoritative list because many compromises are never reported or even discovered. The information is based on accounts published by outside news organizations and researchers.
No More Ransom	National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Center, Kaspersky Lab and Intel Security	Continuously Updated	The online portal offers a one-stop shop for battling ransomware infections.
Information about OPM Cybersecurity Incidents	Office of Personnel Management (OPM)	Continuously Updated	In April 2015, OPM discovered that the personnel data of 4.2 million current and former federal government employees had been stolen. Information such as full name, birth date, home address, and Social Security numbers was affected. While investigating this incident, in early June 2015, OPM discovered that additional information had been compromised, including background investigation records of current, former, and prospective federal employees and contractors.

Chronology of Data Breaches, Security Breaches 2005 to the Present	Privacy Rights Clearinghouse (PRC)	Continuously Updated	The listed (U.S.-only) data breaches have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. This list is not a comprehensive compilation of all breach data. Most of the information is obtained from verifiable media stories, government websites (e.g., state Attorneys General, such as the California AG's breach website), or blog posts with information pertinent to the breach in question.
Criminal Underground Economy Series	Trend Micro	Continuously Updated	A review of various cybercrime markets around the world.
Global Botnet Map	Trend Micro	Continuously Updated	Trend Micro continuously monitors malicious network activities to identify command-and-control (C&C) servers and help increase protection against botnet attacks. The real-time map indicates the locations of C&C servers and victimized computers they control that have been discovered in the previous six hours.
The Equifax Data Breach: What to Do	FTC	September 8, 2017	FTC information on what to do after the Equifax data breach, including information how to set up a credit freeze and/or fraud alert.
Data Integrity: Recovering from Ransomware and Other Destructive Events (DRAFT)	NIST	September 6, 2017	Data integrity incidents, such as ransomware, destructive malware, malicious insider activity, and even honest mistakes, can compromise enterprise information, including emails, employee records, financial records, and customer data. (456 pages)
The FDIC's Processes for Responding to Breaches of Personally Identifiable Information	FDIC Inspector General	September 2017	An FDIC audit found that protocols for responding to a data breach aren't being followed, even as the agency has faced dozens of security incidents in the past two years. The audit stemmed from a series of data breaches at the FDIC over nearly two years, from January 2015 to December 2016. Overall the agency has confirmed or suspects that it was compromised 54 times within that time period. The Office of Inspector General selected 18 of those breaches to evaluate for the audit. (51 pages)
The CERT Guide to Coordinated Vulnerability Disclosure	Carnegie Mellon	August 2017	This document is intended to serve as a guide to those who want to initiate, develop, or improve their own CVD capability. In it, the reader will find an overview of key principles underlying the CVD process, a survey of CVD stakeholders and their roles, and a description of CVD process phases, as well as advice concerning operational considerations and problems that may arise in the provision of CVD and related services. (121 pages)
Social Security Numbers: OMB	GAO	July 27, 2017	GAO was asked to review federal government

Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display			efforts to reduce the collection and use of SSNs. This report examines (1) what governmentwide initiatives have been undertaken to assist agencies in eliminating their unnecessary use of SSNs and (2) the extent to which agencies have developed and executed plans to eliminate the unnecessary use and display of SSNs and have identified challenges associated with those efforts.
Highlights of a Forum: Combating Synthetic Identity Fraud	GAO	July 26, 2017	According to experts, synthetic identity fraud (SIF) has grown significantly in the last five years and has resulted in losses exceeding hundreds of millions of dollars to the financial industry in 2016. A key component of synthetic identities is SSNs—the principal identifier in the credit reporting system. GAO convened and moderated a diverse panel of 14 experts on February 15, 2017 to discuss: how criminals create synthetic identities; the magnitude of the fraud; and issues related to preventing and detecting SIF and prosecuting criminals. (33 pages)
Counting the Cost: Cyber Exposure Decoded	Lloyd's of London	July 10, 2017	Lloyd's Class of Business team estimates that the global cyber market is worth between $3 billion and $3.5 billion. Despite this growth, insurers' understanding of cyber liability and risk aggregation is an evolving process as experience and knowledge of cyber-attacks grows. (56 pages)
2017 Cost of Data Breach Study: Global Overview	Ponemon and IBM	June 28, 2017	According to the report, the average total cost of data breach for the 419 companies participating in the research study decreased from $4.00 to $3.62 million. The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased from $158 in 2016 to $141 in this year's study. However, despite the decline in the overall cost, companies in this year's study are having larger breaches. (35 pages)
2016 Internet Crime Report	Internet Crime Complaint Center's (IC3)	June 21, 2017	IC3 is a joint project of the National White Collar Crime Center and the FBI. In 2016, IC3 received a total of 298,728 complaints with reported losses in excess of $1.3 billion. This past year, the top three crime types reported by victims were non-payment and nondelivery, personal data breach, and payment scams. (28 pages)
Stateless Attribution: Toward International Accountability in Cyberspace	RAND	June 2017	This report reviews the state of cyber attribution and examines alternative options for producing standardized and transparent attribution that may overcome concerns about credibility. In particular, this exploratory work considers the value of an independent, global organization whose mission consists of investigating and publicly attributing major cyber attacks. (64 pages)
Worldwide DDoS Attacks & Cyber Insights Research Report	Neustar	May 2, 2017	Public and private organizations globally are getting slower at detecting and responding to distributed denial of service (DDoS) attacks as

			they become larger and more complex, new research shows. More than half of organizations surveyed in a global study reported taking three hours or more to detect a DDoS attack on their websites in the past year. Forty-eight percent said that they take at least three hours to respond to such an attack. (52 pages)
Data Breach Digest: Perspective is Reality	Verizon	April 26, 2017	In the Data Breach Digest, we share some of our most interesting cases—anonymized of course—so you can learn from the lessons of others. Our 16 cybercrime case studies cover the most lethal and prevalent threats you face—from partner misuse to sophisticated malware. We set out the measures you can take to better defend your organization and respond quickly if you are a victim of an attack. (100 pages)
Data Breach Investigative Report (registration required)	Verizon	April 27, 2017	The latest report examined 42,068 incidents and 1,935 breaches from 84 countries, drawing from the collective data of 65 organizations. Cyber espionage accounts for 21% of breaches, still far behind the 73% hat are financially motivated. Breaches are heavily concentrated in three sectors: financial, health care, and public sector. (76 pages)
2017 Internet Security Threat Report (registration required)	Symantec	April 26, 2017	Cyberattackers are seeking bigger financial hauls, targeting massive dollar amounts, and more than tripling their asking price via ransomware from 2015 to 2016. In 2015, ransomware demands averaged $294, but that jumped to $1,077 in 2016. The probable cause is that victims are paying up: globally, 34% paid the ransom, and in the United States, 64% did. (77 pages)
The Cyber-Value Connection: Revealing the link between cyber vulnerability	CGI/Oxford Economics	April 2017	The report looks at the reduction in company value that arises from a cyber breach, vividly demonstrating how a severe incident leads to a decline in share price. To ensure rigor and independence, CGI commissioned Oxford Economics to develop a robust econometric model using a "difference in differences" technique to isolate the damage caused to company value by a cyber breach from other movements in the market. (28 pages)
Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud	GAO	March 30, 2017	GAO was asked to examine issues related to identity theft services and their usefulness. The report examines, among other objectives, (1) the potential benefits and limitations of identity theft services and (2) factors that affect government and private-sector decisionmaking about them. GAO reviewed products, studies, laws, regulations, and federal guidance and contracts, and interviewed federal agencies, consumer groups, industry stakeholders, and eight providers selected because they were large market participants. (70 pages)
Zero Days, Thousands of Nights: The	RAND	March 13,	This report provides findings from real-world

Life and Times of Zero-Day Vulnerabilities and Their Exploits		2017	zero-day vulnerability and exploit data that could augment conventional proxy examples and expert opinion, complement current efforts to create a framework for deciding whether to disclose or retain a cache of zero-day vulnerabilities and exploits, inform ongoing policy debates regarding stockpiling and vulnerability disclosure, and add extra context for those examining the implications and resulting liability of attacks and data breaches for U.S. consumers, companies, insurers, and for the civil justice system broadly. (133 pages)
IBM X-Force Threat Intelligence Index 2017: The Year of the Mega-Breach	IBM	March 2017	In 2016, more than 4 billion records were leaked worldwide, exceeding the combined total from the two previous years, according to a report from IBM Security. The leaked documents comprised the usual credit cards, passwords, and personal health information, but the report also notes a shift in cybercriminal strategies, finding a number of significant breaches were related to unstructured data such as email archives, business documents, intellectual property, and source code. (30 pages)
The Web of Vulnerabilities: Hunters, Hackers, Spies, and Criminals	*Christian Science Monitor's* Passcode team and Northwestern University's Medill School of Journalism	February 10, 2017	In a joint multimedia project between *The Christian Science Monitor's* Passcode team and Northwestern University's Medill School of Journalism, they explore the growing arms race to discover software vulnerabilities and what it means for national security and everyone's digital privacy and safety.
2017 Identity Fraud: Securing the Connected Life (press release)	Javelin Strategy & Research	February 2017	The study revealed that the number of identity fraud victims increased by 16% (rising to 15.4 million U.S. consumers) in the last year, a record high since Javelin Strategy & Research began tracking identity fraud in 2003. The study found that despite the efforts of the industry, fraudsters successfully adapted to net two million more victims this year with the amount fraudsters took rising by nearly $1 billion to $16 billion. (6 pages)
In 2017, The Insider Threat Epidemic Begins	Institute for Critical Infrastructure Technology	February 2017	The report offers a comprehensive analysis of the Insider Threat Epidemic, including research on (1) Characterizing Insider Threats (the insider threat cyber "kill chain," non-malicious insider threats, malicious insider threats) (2) The Insider Threat Debate (3) Policies, Procedures, and Guidelines to Combat Insider Threats (4) Non-Technical Controls (5) Technical Controls. (52 pages)
Risk and Anxiety: A Theory of Data Breach Harms	Texas Law Review	December 14, 2016	The essay examines why courts have struggled when dealing with harms caused by data breaches. The difficulty largely stems from the fact that data breach harms are intangible, risk-oriented, and diffuse. The report explores how existing legal foundations support the recognition of such harm. It demonstrates how courts can assess risk and anxiety in a concrete and coherent way.
Verisign Distributed Denial of Service	Verisign	December	Provides a view into attack statistics and

Trends Report		2016	behavioral trends during the third quarter of 2016: 81% of attacks peaked over 1 Gbps' 82% increase in attack size year over year; 59% of attacks used multiple attack types. (12 pages)
Department Releases Intake and Charging Policy for Computer Crime Matters	Department of Justice	October 25, 2016	In the course of litigation, DOJ released the policy under which it chooses whether to bring charges under the Computer Fraud and Abuse Act. As set forth in the memorandum, prosecutors must consider a number of factors to ensure that charges are brought only in cases that serve a substantial federal interest.
Data Breach Response: A Guide for Businesses	Federal Trade Commission (FTC)	October 25, 2016	The guidance document provides a basic checklist to help identify the general legal coverage for various types of data and point businesses to the relevant legal standards. It also includes a model notice letter for individuals whose Social Security numbers may have been breached. (16 pages)
IoT Devices as Proxies for Cybercrime	Krebs on Security	October 13, 2016	The post looks at how crooks are using hacked IoT devices as proxies to hide their true location online as they engage in a variety of other types of cybercriminal activity—from frequenting underground forums to credit card and tax refund fraud.
Examining the Costs and Causes of Cyber Incidents	RAND	October 10, 2016	Researchers found that the typical cost of a breach was about $200,000 and that most cyber events cost companies less than 0.4% of their annual revenues. The $200,000 cost was roughly equivalent to a typical company's annual information security budget. (15 pages)
From the Trenches: Current Status of Security and Risk in the Financial Sector	SANS Institute	October 6, 2016	According to a recent SANS survey, some 55% of financial services firms report ransomware as the top attack threat, followed by phishing (50%), which previously held the top spot. More than 32% of financial firms say they've lost anywhere from $100,000 to $500,000 due to ransomware attacks.
2016 Internet Organised Crime Threat Assessment (IOCTA)	Europol	September 28, 2016	The IOCTA reports a continuing and increasing acceleration of the security trends observed in previous assessments. The additional increase in volume, scope, and financial damage combined with the asymmetric risk that characterizes cybercrime has reached such a level that in some EU countries cybercrime may have surpassed traditional crime in terms of reporting. (72 pages)
The Rising Face of Cyber Crime: Ransomware	BitSight	September 21, 2016	Ransomware attacks on government agencies around the world have tripled in the past year. Government entities are second most likely to be targeted by ransomware attacks, following only the education sector. About 4% of government agencies had been exposed to Nymaim, and 3% to Locky, both ransomware strains. Of all industries, government had the second lowest security rating and the highest ransomware attack rate. (11 pages)

Ransomware Victims Urged to Report Infections to Federal Law Enforcement	FBI	September 15, 2016	The FBI is requesting victims reach out to their local FBI office or file a complaint with the Internet Crime Complaint Center, at http://www.IC3.gov, with ransomware infection details (as detailed on the website).
Workshop on Data Breach Aftermath and Recovery for Individuals and Institutions	National Academies Press	September 2016	In January 2016, the National Academies of Sciences, Engineering, and Medicine hosted the Workshop on Data Breach Aftermath and Recovery for Individuals and Institutions. Participants examined existing technical and policy remediations, and they discussed possible new mechanisms for better protecting and helping consumers in the wake of a breach. Speakers were asked to focus on data breach aftermath and recovery and to discuss ways to remediate harms from breaches. The publication summarizes the presentations and discussions from the workshop. (67 pages)
Examining the costs and causes of cyber incidents	Journal of Cybersecurity	August 25, 2016	Researchers examined a sample of more than 12 000 cyber events that include data breaches, security incidents, privacy violations, and phishing crimes. The findings suggest that public concerns regarding the increasing rates of breaches and legal actions may be excessive compared with the relatively modest financial impact to firms that suffer these events. Specifically, they found that the cost of a typical cyber incident is less than $200 000 (about the same as the firm's annual IT security budget), which represents only 0.4% of a firm's estimated annual revenues. (15 pages)
Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications	New America	July 28, 2016	The report offers five initial policy recommendations to ensure that more vulnerabilities are discovered and patched sooner: (1) The U.S. government should minimize its participation in the vulnerability market, because it is the largest buyer in a market that discourages researchers from disclosing vulnerabilities to be patched; (2) The U.S. government should establish strong, clear procedures for government disclosure of the vulnerabilities it buys or discovers, with a heavy presumption toward disclosure; (3) Congress should establish clear rules of the road for government hacking to better protect cybersecurity and civil liberties; (4) Government and industry should support bug bounty programs as an alternative to the vulnerabilities market and investigate other innovative ways to foster the disclosure and prompt patching of vulnerabilities; and (5) Congress should reform computer crime and copyright laws, and agencies should modify their application of such laws to reduce the legal chill on legitimate security research. (40 pages)
Second Interim Status Report on the U.S. Office of Personnel	OPM	May 18, 2016	The report finds that funding for the troubled IT security upgrades project remains an issue in part

Management's (OPM) Infrastructure Improvement Project – Major IT Business Case			because of the agency's poor planning. The inspector general finds the agency still lacks a "realistic budget" for the massive upgrade. (12 pages)
Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information	RAND Corp.	April 20, 2016	Key findings include (1) 26% of respondents, or an estimated 64 million U.S. adults, recalled a breach notification in the past 12 months; (2) 44% of those notified were already aware of the breach; (3) 62% of respondents accepted offers of free credit monitoring; (4) only 11% of respondents stopped dealing with the affected company following a breach; (5) 32% of respondents reported no costs of the breach and any inconvenience it garnered, while, among those reporting some cost, the median cost was $500; and (6) 77% of respondents were highly satisfied with the company's post-breach response.
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.
Combatting the Ransomware Blitzkrieg: The Only Defense is a Layered Defense, Layer One: Endpoint Security	The Institute for Critical Infrastructure Technology	April 2016	The report introduces the ins and outs of the more prevalent ransomware variants as well as other endpoints vulnerable to ransomware attacks, such as SCADA/ICS, IoT, cars, cloud, servers, specialized hardware, personal computers, and the most easily exploitable vulnerability, the human. (27 pages)
2016 Data Breach Investigations Report	Verizon	April 2016	Provides analysis and statistics on worldwide data breaches. "In 93% of cases, it took attackers minutes or less to compromise systems. Organizations, meanwhile, took weeks or more to discover that a breach had even occurred—and it was typically customers or law enforcement that sounded the alarm, not their own security measures." (85 pages)
A Look Inside Cybercriminal Call Centers	Krebs on Security	January 11, 2016	Crooks who make a living via identity theft schemes, dating scams, and other con games often run into trouble when presented with a phone-based challenge that requires them to demonstrate mastery of a language they do not speak fluently. Enter the criminal call center, which allows scammers to outsource those calls to multilingual men and women who can be hired to close the deal.
Target Settlement Memorandum	U.S. District Court, District of Minnesota	December 2, 2015	Target Corporation has agreed to pay financial institutions almost $40 million to settle a class-action suit related to its massive 2013 data breach. The proposed settlement of up to $39,357,938.38

			will apply to all U.S. financial institutions that issued payment cards put at risk as a result of the data breach. (20 pages)
The Cyberwar is On (Special Issue)	*The Agenda* (Politico)	December 2015	The cyber issue of *The Agenda* magazine contents include "Why Politicians can't Handle Cyber," "Inside the NSA's Hunt for Hackers," "America's Secret Arsenal," " The Biggest Hacks (We Know About)," "Survey: What Keeps America's Computer Experts Up at Night?," The 'Electronic Pearl Harbor'," " Our Best Frenemy, Time for a Ralph Nader Moment," "The Crypto Warrior," and "America's CIO."
Fiscal Year 2015 Top Management Challenges	Office of Personnel Management (OPM), Office of Inspector General (OIG)	October 30, 2015	See Internal Challenges section (pp. 15-22) 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)
With Stolen Cards, Fraudsters Shop to Drop	Krebs on Security	September 28, 2015	Fraudsters have perfected the reshipping service, a criminal enterprise that allows card thieves and the service operators to essentially split the profits from merchandise ordered with stolen credit and debit cards.
Drops for Stuff: An Analysis of Reshipping Mule Scams	Federal Bureau of Investigation (FBI), University of CA Santa Barbara, Stony Brook University, Krebs on Security, University College London	September 23, 2015	In reshipping scams, cybercriminals purchase high-value or high-demand products from online merchants using stolen payment instruments, and then ship the items to a credulous citizen. This person, who has been recruited by the scammer under the guise of "work-from-home" opportunities, then forwards the received products to the cybercriminals, most of whom are located overseas. Once the goods reach the cybercriminals, they are then resold on the black market for an illicit profit. (12 pages)
Follow the Data: Dissecting Data Breaches and Debunking Myths	Trend Micro	September 22, 2015	Trend Micro's Forward-Looking Threat Research (FTR) Team has taken 10 years (2005-2015) of information on data breaches in the United States from the Privacy Rights Clearinghouse (PRC) and subjected it to detailed analysis to better understand the real story behind data breaches and their trends. (51 pages)
Timeline: Government Data Breaches	Government Executive	July 6, 2015	The timelines are based mainly on testimony from OPM Director Catherine Archuleta and Andy Ozment, assistant secretary for Cybersecurity and Communications at DHS, supplemented by information from news reports.
2015 Cost of Data Breach Study:	Ponemon Institute	May 27,	The average cost of a breach was up worldwide in

Global Analysis	and IBM	2015	2014, with U.S. firms paying almost $1.5 million more than the global average. In the United States, a data breach costs organizations on average $5.85 million (the highest of the 10 nations analyzed), up from $5.4 million in 2013. Globally, the cost of a breach is up 15% this year to $3.5 million. The United States likewise had the highest cost per record stolen, at $201, up from $188 last year. The country also led in terms of size of breaches recorded: U.S. companies averaged 29,087 records compromised in 2014. (Free registration required to download.) (31 pages)
Meet 'Tox': Ransomware for the Rest of Us	McAfee Labs	May 23, 2015	The packaging of malware and malware-construction kits for cybercrime "consumers" has been a long-running trend. Various turnkey kits that cover remote access plus botnet plus stealth functions are virtually anywhere. Ransomware, though very prevalent, has not yet appeared in force in easy-to-deploy kits. However, Tox is now available free.
2014 Internet Crime Report	Internet Crime Complaint Center (IC3)	May 19, 2015	IC3, a joint project of the National White Collar Crime Center and the FBI, received 269,422 complaints last year consisting of a wide array of scams affecting victims across all demographic groups. In 2014, victims of Internet crimes in the United States lost more than $800 million. On average, approximately 22,000 complaints were received each month. (48 pages)
Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data	Ponemon Institute	May 2015	A rise in cyberattacks against doctors and hospitals is costing the U.S. health-care system $6 billion a year as organized criminals who once targeted retailers and financial firms increasingly go after medical records. Criminal attacks are up 125% compared with five years ago lost laptops was the leading threat. The study also found most organizations are unprepared to address new threats and lack adequate resources to protect patient data. (7 pages)
Best Practices for Victim Response and Reporting of Cyber Incidents	Department of Justice (DOJ)	April 29, 2015	DOJ issued new guidance for businesses on best practices for handling cyber incidents. The guidance is broken down into what companies should do—and should not do—before, during, and after an incident. The recommendations include developing an incident response plan, testing it, identifying highly sensitive data and risk management priorities, and connecting with law enforcement and response firms in advance. (15 pages)
2014 Global Threat Intel Report	CrowdStrike	February 6, 2015	The report summarizes CrowdStrike's year-long daily scrutiny of more than 50 groups of cyber threat actors, including 29 different state-sponsored and nationalist adversaries. Key findings explain how financial malware changed the threat landscape and point of sale malware became increasingly prevalent. The report also profiles a number of new and sophisticated

			adversaries from China and Russia. (Free registration required.)
Unique in the Shopping Mall: on the Reidentifiability of Credit Card Metadata	*Science Magazine*	January 30, 2015	Massachusetts Institute of Technology (MIT) scientists showed they can identify an individual with more than 90% accuracy by looking at just four purchases; three if the price is included—and this is after companies "*anonymized*" the transaction records, saying they wiped away names and other personal details. (5 pages)
Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat	FBI	January 20, 2015	Ransomware scams involve a type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom—anywhere from hundreds to thousands of dollars—is paid. The site offers information on the FBI's and federal, international, and private-sector partners' proactive steps to neutralize some of the more significant ransomware scams through law enforcement actions against major botnets.
Exploit This: Evaluating the Exploit Skills of Malware Groups	Sophos Labs Hungary	January 2015	Researchers evaluated the malware and advanced persistent threat (APT) campaigns of several groups that all leveraged a particular exploit—a sophisticated attack against a specific version of Microsoft Office. The report found that none of the groups were able to modify the attack enough to infect other versions of Office, even though several versions were theoretically vulnerable to the same type of attack. Despite the aura of skill and complexity that seems to surround APTs, they are much less sophisticated than they are given credit for. (26 pages)
The Cost of Malware Containment	Ponemon Institute	January 2015	A survey of more than 600 U.S. IT security practitioners found that in a typical week, organizations receive an average of nearly 17,000 malware alerts; only 19% are deemed reliable or worthy of action. Compounding the problem, respondents believe their prevention tools miss 40% of malware infections in a typical week. (Free registration required.)
Addressing the Cybersecurity Malicious Insider Threat	Schluderberg, Larry (Utica College Master's Thesis)	January 2015	"The purpose of this research was to investigate who constitutes Malicious Insider (MI) threats, why and how they initiate attacks, the extent to which MI activity can be modeled or predicted, and to suggest risk mitigation strategies. The results reveal that addressing the Malicious Insider threat is much more than just a technical issue. Dealing effectively with the threat involves managing the dynamic interaction between employees, their work environment and work associates, the systems with which they interact, and organizational policies and procedures." (80 pages)
The Underground Hacker Markets are Booming with Counterfeit Documents,	Dell Secure Works	December 2014	Researchers examined dozens of underground hacker markets and found that business is

Premiere Credit Cards, Hacker Tutorials, and 1000% Satisfaction Guarantees			booming. Prices have gone down for many items and the offerings have expanded. According to the report, "Underground hackers are monetizing every piece of data they can steal or buy and are continually adding services so other scammers can successfully carry out online and in-person fraud." (16 pages)
What Happens When You Swipe Your Card?	*60 Minutes*	November 30, 2014	From the script for the segment "Swiping Your Card": "Sophisticated cyberthieves steal your credit card information. Common criminals buy it and go on shopping sprees—racking up billions of dollars in fraudulent purchases. The cost of the fraud is calculated into the price of every item you buy. When computer crooks swipe your card number, we all end up paying the price. 2014 is becoming known as the 'year of the data breach.'"
Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation	Heritage Foundation	October 27, 2014	A list of federal government cybersecurity breaches and failures, most of which occurred during 2013 and 2014. The list is part of a continuing series published by Heritage that serves as a long-term compilation of open-source data about federal cybersecurity breaches dating back to 2004.
2014 Cost of Cybercrime Global Report	Hewlett-Packard Enterprise Security and the Ponemon Institute	October 8, 2014	This 2014 global study of U.S.-based companies, which spanned seven nations, found that over the course of a year, the average cost of cybercrime climbed by more than 9% to $12.7 million for companies in the United States, up from $11.6 million in the 2013 study. The average time to resolve a cyberattack is also rising, climbing to 45 days from 32 days in 2013. (30 pages) (Email registration required.)
The Deep Web (Special Issue)	*The Kernel*	September 28, 2014	A special issue devoted to the Deep Web, Tor, Silk Road, black markets, etc.
How Consumers Foot the Bill for Data Breaches (infographic)	NextGov.com	August 7, 2014	More than 600 data breaches occurred in 2013 alone, with an average organizational cost of more than $5 million. But in the end, it is the customers who are often picking up the tab, from higher retail costs to credit card reissue fees.
Is Ransomware Poised for Growth?	Symantec	July 14, 2014	Ransomware usually masquerades as a virtual "wheel clamp" for the victim's computer. For example, pretending to be from the local law enforcement, it might suggest the victim had been using the computer for illicit purposes and claim that to unlock his or her computer the victim would have to pay a fine—often between $100 and $500. The use of Ransomware escalated in 2013, with a 500% (sixfold) increase in attacks between the start and end of the year.
iDATA: Improving Defences Against Targeted Attack	Centre for the Protection of National Infrastructure (UK)	July 2014	The iDATA program consists of a number of projects aimed at addressing threats posed by nation-states and state-sponsored actors. iDATA has resulted in several outputs for the

			cybersecurity community. The document provides a description of the iDATA program and a summary of the reports. (8 pages)
Cyber Risks: The Growing Threat	Insurance Information Institute	June 27, 2014	Although cyber risks and cybersecurity are widely acknowledged to be serious threats, many companies today still do not purchase cyber risk insurance. Insurers have developed specialist cyber insurance policies to help businesses and individuals protect themselves from the cyber threat. Market intelligence suggests that the types of specialized cyber coverage being offered by insurers are expanding in response to this fast-growing market need. (27 pages)
Hackers Wanted: An Examination of the Cybersecurity Labor Market	RAND Corporation	June 24, 2014	RAND examined the current status of the labor market for cybersecurity professionals—with an emphasis on their being employed to defend the United States. This effort was in three parts: first, a review of the literature; second, interviews with managers and educators of cybersecurity professionals, supplemented by reportage; and third, an examination of the economic literature about labor markets. RAND also disaggregated the broad definition of *cybersecurity professionals* to unearth skills differentiation as relevant to this study. (110 pages)
Big Data and Innovation, Setting The Record Straight: De-identification Does Work	Information Technology and Innovation Foundation and the Information and Privacy Commissioner, Ontario, Canada	June 16, 2014	The paper examines a select group of articles that are often referenced in support of the myth that de-identified data sets are at risk of re-identifying individuals through linkages with other available data. It examines the ways in which the academic research referenced has been misconstrued and finds that the primary reason for the popularity of these misconceptions is not factual inaccuracies or errors within the literature but rather a tendency on the part of commentators to overstate or exaggerate the risk of re-identification. (13 pages)
Net Losses: Estimating the Global Cost of Cybercrime	Center for Strategic and International Studies and McAfee	June 2014	The report explores the economic impact of cybercrime, including estimation, regional variances, IP theft, opportunity and recovery costs, and the future of cybercrime. (24 pages)
2014 U.S. State of Cybercrime Survey	Pricewaterhouse Coopers, *CSO Magazine*, the CERT Division of the Software Engineering Institute at Carnegie Mellon University, and the U.S. Secret Service	May 29, 2014	The cybersecurity programs of U.S. organizations do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries. This year, three out of four (77%) respondents to the survey had detected a security event in the past 12 months, and more than one-third (34%) said the number of security incidents detected had increased over the previous year. (21 pages)
Privileged User Abuse and The Insider Threat	Ponemon Institute and Raytheon	May 21, 2014	The report looks at what companies are doing right and the vulnerabilities that need to be addressed with policies and technologies. One problematic area is the difficulty in actually

			knowing if an action taken by an insider is truly a threat. Sixty-nine percent of respondents say they do not have enough contextual information from security tools to make this assessment, and 56% say security tools yield too many false positives. (32 pages) (Requires free registration to access.)
Online Advertising and Hidden Hazards to Consumer Security and Data Privacy	Senate Permanent Subcommittee on Investigations	May 15, 2014	The report found consumers could expose themselves to malware just by visiting a popular website. It noted that the complexity of the industry made it possible for both advertisers and host websites to defer responsibility and that consumer safeguards failed to protect against online abuses. The report also warned that current practices do not create enough incentives for "online advertising participants" to take preventive measures. (47 pages)
Sharing Cyberthreat Information Under 18 USC § 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, (18 U.S.C. § 2701 et seq.) which prohibits providers from voluntarily disclosing customer information to governmental entities. The white paper says the law does not prohibit companies from divulging data in the aggregate, without any specific details about identifiable customers. (7 pages)
The Target Breach, by the Numbers	Krebs on Security	May 6, 2014	A synthesis of numbers associated with the Target data breach of December 19, 2013 (e.g., number of records stolen, estimated dollar cost to credit unions and community banks, and the amount of money Target estimates it will spend upgrading payment terminals to support Chip-and-PIN enabled cards).
The Rising Strategic Risks of Cyberattacks	McKinsey and Company	May 2014	The authors suggest that companies are struggling with their capabilities in cyber risk management. As highly visible breaches occur with increasing regularity, most technology executives believe they are losing ground to attackers. Organizations large and small lack the facts to make effective decisions, and traditional "protect the perimeter" technology strategies are proving insufficient.
Big Data: Seizing Opportunities, Preserving Values	White House	May 2014	Findings include a set of consumer protection recommendations, such as national data-breach legislation, and a fresh call for baseline consumer-privacy legislation first recommended in 2012. (85 pages)
Russian Underground Revisited	Trend Micro	April 28, 2014	The price of malicious software—designed to enable online bank fraud, identity theft, and other cybercrimes—is falling dramatically in some of the Russian-language criminal markets in which it is sold. Falling prices are a result not of declining demand but rather of an increasingly sophisticated marketplace. The report outlines the products and services being sold and their prices. (25 pages)

Federal Agencies Need to Enhance Responses to Data Breaches	Government Accountability Office (GAO)	April 2, 2014	Major federal agencies continue to face challenges in fully implementing all components of agency-wide information security programs, which are essential for securing agency systems and the information they contain—including personally identifiable information (PII). (19 pages)
A "Kill Chain" Analysis of the 2013 Target Data Breach	Senate Commerce Committee	March 26, 2014	The report analyzes what has been reported to date about the Target data breach, using the *intrusion kill chain* framework, an analytical tool introduced by Lockheed Martin security researchers in 2011 and widely used today by information security professionals in both the public and private sectors. The analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach. (18 pages)
Markets for Cybercrime Tools and Stolen Data	RAND Corporation National Security Research Division and Juniper Networks	March 25, 2014	The report, part of a multiphase study on the future security environment, describes the fundamental characteristics of the criminal activities in cyberspace markets and how they have grown into their current state to explain how their existence can harm the information security environment. (83 pages)
Merchant and Financial Trade Associations Announce Cybersecurity Partnership	Retail Industry Leaders Association	February 13, 2014	Trade associations representing the merchant and financial services industries announced a new cybersecurity partnership. The partnership will focus on exploring paths to increased information sharing, better card security technology, and maintaining the trust of customers. Discussion regarding the partnership was initiated by the Retail Industry Leaders Association and the Financial Services Roundtable.
FTC Statement Marking the FTC's 50th Data Security Settlement	Federal Trade Commission (FTC)	January 31, 2014	The FTC announced its 50th data security settlement. What started in 2002 with a single case applying established FTC Act precedent to the area of data security has grown into an enforcement program that has helped to increase consumer protections and encouraged companies to make safeguarding consumer data a priority. (2 pages)
Worst Practices Guide to Insider Threats: Lessons from Past Mistakes	American Academy of Arts and Sciences	January 2014	The report presents a *worst practices* guide of serious past mistakes regarding insider threats. Although each situation is unique, and serious insider problems are relatively rare, the incidents reflect issues that exist in many contexts and that every security manager should consider. Common organizational practices—such as prioritizing production over security, failure to share information across subunits, inadequate rules or inappropriate waiving of rules, exaggerated faith in group loyalty, and excessive focus on external threats—can be seen in many past failures to protect against insider threats. (32 pages)

ENISA Threat Landscape 2013—Overview of Current and Emerging Cyber-Threats	European Union Agency for Network and Information Security (ENISA)	December 11, 2013	The report is a comprehensive compilation of the top 15 cyber threats assessed in the 2013-reporting period. ENISA has collected more than 250 reports regarding cyber threats, risks, and threat agents. (70 pages)
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 government wide 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)
Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences	Brookings Institution	December 2013	Economic espionage has existed at least since the industrial revolution, but the scope of modern cyber-enabled competitive data theft may be unprecedented. The authors present what they believe is the first economic framework and model to understand the long-run impact of competitive data theft on an economy by taking into account the actual mechanisms and pathways by which theft harms the victims. (18 pages)
Illicit Cyber Activity Involving Fraud	Carnegie Mellon University Software Engineering Institute	August 8, 2013	Technical and behavioral patterns were extracted from 80 fraud cases—67 insider and 13 external—that occurred between 2005 and the present. These cases were used to develop insights and risk indicators to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage malicious insider activity within the banking and finance sectors. (28 pages)
The Economic Impact of Cybercrime and Cyber Espionage	Center for Strategic and International Studies (CSIS)	July 22, 2013	According to CSIS, losses to the United States (the country in which data is most accessible) may reach $100 billion annually. The cost of cybercrime and cyber espionage to the global economy is some multiple of this, likely measured in hundreds of billions of dollars. (20 pages)
Cyber-Crime, Securities Markets, and Systemic Risk	World Federation of Exchanges and the International Organization of Securities Commissions	July 16, 2013	The report explores the nature and extent of cybercrime in securities markets and the potential systemic risk aspects of this threat. It presents the results of a survey to the world's exchanges on their experiences with cybercrime, cybersecurity practices, and perceptions of the risk. (59 pages)
Remaking American Security: Supply Chain Vulnerabilities and National Security Risks Across the U.S.	Alliance for American Manufacturing	May 2013	Reportedly because the supply chain is global, it makes sense for U.S. officials to cooperate with other nations to ward off cyberattacks. Increased

Defense Industrial Base			international cooperation to secure the integrity of the global IT system is a valuable long-term objective. (355 pages)
Comprehensive Study on Cybercrime	United Nations Office on Drugs and Crime	February 2013	The study examined the problem of cybercrime from the perspective of governments, the private sector, academia, and international organizations. It presents its results in eight chapters, covering (1) Internet connectivity and cybercrime; (2) the global cybercrime picture; (3) cybercrime legislation and frameworks; (4) criminalization of cybercrime; (5) law enforcement and cybercrime investigations; (6) electronic evidence and criminal justice; (7) international cooperation in criminal matters involving cybercrime; and (8) cybercrime prevention. (320 pages)
Does Cybercrime Really Cost $1 Trillion?	ProPublica	August 1, 2012	In a news release to announce its 2009 report, *Unsecured Economies: Protecting Vital Information*, computer security firm McAfee estimated a $1 trillion global cost for cybercrime. The number does not appear in the report itself. This estimate is questioned even by the three independent researchers from Purdue University whom McAfee credits with analyzing the raw data from which the estimate was derived. An examination by ProPublica has found new grounds to question the data and methods used to generate these numbers, which McAfee and Symantec say they stand behind.
Proactive Policy Measures by Internet Service Providers against Botnets	Organization for Economic Co-operation and Development (OECD)	May 7, 2012	The report analyzes initiatives in a number of countries through which end-users are notified by Internet service providers (ISPs) when their computers are identified as being compromised by malicious software and encouraged to take action to mitigate the problem. (25 pages)
Developing State Solutions to Business Identity Theft: Assistance, Prevention and Detection Efforts by Secretary of State Offices	National Association of Secretaries of State (NASS)	January 2012	The white paper is the result of efforts by the 19-member NASS Business Identity Theft Task Force to develop policy guidelines and recommendations for state leaders dealing with identity fraud cases involving public business records. (23 pages)
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines	SANS Institute	October 3, 2011	The 20 security measures are intended to focus agencies' limited resources on plugging the most common attack vectors. (77 pages)
Revealed: Operation Shady RAT: an Investigation Of Targeted Intrusions Into 70+ Global Companies, Governments, and Non-Profit Organizations During the Last 5 Years	McAfee	August 2, 2011	A cyber-espionage operation lasting many years penetrated 72 government and other organizations, most of them in the United States, and has copied everything from military secrets to industrial designs, according to technology security company McAfee. (See page 4 for the types of compromised parties, page 5 for the geographic distribution of victim's country of origin, pages 7-9 for the types of victims, and pages 10-13 for the number of intrusions for 2007-2010). (14 pages)

The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis Based on Spam Data	Organisation for Economic Co-operation and Development (OECD)	November 12, 2010	The working paper considers whether ISPs can be critical control points for botnet mitigation, how the number of infected machines varies across ISPs, and why. (31 pages)
Untangling Attribution: Moving to Accountability in Cyberspace (Testimony)	Council on Foreign Relations	July 15, 2010	Robert K. Knake's testimony before the House Committee on Science and Technology on the role of attack attribution in preventing cyberattacks and how attribution technologies can affect the anonymity and privacy of Internet users. (14 pages)
Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities	National Research Council	2009	The report explores important characteristics of cyberattacks. It describes the current international and domestic legal structure as it might apply to cyberattacks and considers analogies to other domains of conflict to develop relevant insights. (368 pages)

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are for documents; other cited resources are webpages.

Table 2. National Security, Cyber Espionage, and Cyberwar

(includes Stuxnet, Dark Web/Dark Net)

Title	Source	Date	Notes
Cybersecurity Legislation	International Telecommunications Union	Continuously Updated	An integral and challenging component of any national cybersecurity strategy is the adoption of regionally and internationally harmonized, appropriate legislation against the misuse of information and communication technologies (ICTs) for criminal or other purposes.
Cyberthreat: Real-Time Map	Kaspersky Labs	Continuously Updated	Kaspersky Labs has launched an interactive cyber threat map that lets viewers see cybersecurity incidents as they occur around the world in real time. The interactive map includes malicious objects detected during on-access and on-demand scans, email and web antivirus detections, and objects identified by vulnerability and intrusion detection subsystems.
Cyberwarfare	RAND	Continuously Updated	Explore RAND reports on cyberwarfare by product type (research, blog, multimedia, event, etc.) or author. Featured reports are at the top of the page.
Too Connected To Fail: How Attackers Can Disrupt the Global Internet, Why It Matters, And What We Can Do About It	Belfer Center for Science and International Affairs (Harvard)	May 2017	This paper examines attacks on core internet infrastructure through a lens of national security and nation state conflict. Most analyses have focused on the ability of non-state actors to use these tools to exact

			ransom or commit mischief. While these are real concerns, an examination of these attacks' applicability in nation state conflict has been missing. (54 pages)
Cyber Compellence: Applying Coercion in the Information Age	Marine Corps University and Northeastern University, presented at the Annual International Studies Association Meeting, Baltimore, Maryland	April 25, 2017	The paper reviews how state actors applied cyber instruments to coerce adversaries between 2000 to 2014 differentiating between cyber disruption, espionage, and degradation. Cyber disruption and espionage methods seem to achieve their goals of gathering intelligence and signaling through harassment, but do not result in an observable behavioral change in the target in the near-term. Only on limited occasion, usually associated with US activity in cyberspace, does cyber coercion, often in the form of degradation, result in concessions. The idea of quick victory in the cyber domain remains elusive. (27 pages)
Bad Bots: The Weaponization of Social Media	College of William and Mary; Project on International Peace and Security	April 2017	In the next several years, hostile states or non-state actors will accelerate their use of social media bots to undermine democracy, recruit terrorists, disrupt markets, and stymie open-source intelligence collection. This report conducts an alternative futures analysis in order to help policymakers identify options to mitigate the threats of social media bots. In the worst-case and most-likely scenario, a technological stalemate between bots and bot-detection leads to a false sense of confidence in social media information, which allows for breakthroughs in bot technology to create disruptions until bot-detection technology advances. (23 pages)
Strategic Aspects of Cyberattack, Attribution, and Blame	Proceedings of the National Academy of Sciences	March 14, 2017	Attribution of cyberattacks has strategic and technical components. A formal model incorporates both elements and shows the conditions under which it is rational to tolerate an attack and when it is better to assign blame publicly. The model applies to a wide range of conflicts and provides guidance to policymakers about which parameters must be estimated to make a sound decision about attribution and blame. It also draws some surprising conclusions about the risks of asymmetric technical attribution capabilities. (12 pages)
Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits	RAND	March 13, 2017	The report provides findings from real-world zero-day vulnerability and exploit data that could augment conventional proxy examples and expert opinion, complement current efforts to create a framework for deciding whether to disclose or retain a cache of zero-day vulnerabilities and exploits, inform ongoing policy debates regarding stockpiling and vulnerability disclosure, and add extra context for those examining the implications

			and resulting liability of attacks and data breaches for U.S. consumers, companies, insurers, and for the civil justice system broadly. (133 pages)
Snapshot: Turning Back DDoS Attacks	DHS Science and Technology, Homeland Security Advanced Research Projects Agency's Cyber Security Division (CSD)	February 16, 2017	CSD's Distributed Denial of Service Defense (DDoSD) project is spearheading a three-pronged approach to shift the advantage to network infrastructure defenders. The project's two primary focuses are on increasing deployment of best practices to slow attack scale growth and defending networks against one Tbps attack through development of collaboration tools that can be used by medium-size organizations. A third part of the project addresses other types of denial of service attacks, such as those against 911 and Next Generation 911 emergency management systems.
Task Force on Cyber Deterrence	Defense Science Board	February 2017	The U.S. military lacks the cyber capabilities to defend against potential attacks against financial systems, telecommunications systems, and other elements of critical infrastructure launched by Russia or China. Furthermore, the U.S. military's dependence on IT makes it vulnerable to attacks that could diminish its capabilities to respond to such attacks. The task force recommends that the Pentagon develop a second-strike capability that is cyber-resilient. (44 pages)
The Enemy Has a Voice: Understanding Threats to Inform Smart Investment in Cyber Defense	New America	February 2017	The report discusses the general concept of cyber threat intelligence (CTI) and how this powerful concept can reduce "offensive dominant" nature of cybersecurity and describe various types of such information. The report outlines challenges with cyber threat intelligence going forward and proposes policy ideas that can help lead to improved access to such information across a variety of organizations. (16 pages)
Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness	MITRE Corp.	February 2017	Cyber Prep 2.0 focuses on advanced threats and corresponding elements of organizational strategy and includes material related to conventional cyber threats. Cyber Prep 2.0 can be used in standalone fashion, or it can be used to complement and extend the use of other, more detailed frameworks (e.g., the NIST [National Institute of Standards and Technology] Cybersecurity Framework) and threat models.
The U.S. Government and Zero-Day Vulnerabilities: from Pre-Heartbleed to Shadow Brokers	Columbia Univ. Journal of International Affairs	November 2016	Government agencies currently submit zero days they discover to an interagency Vulnerability Equities Process headed by the National Security Council. The review examines questions such as how likely criminals and foreign adversaries are to discover the vulnerability and how much

			damage they could do if they did discover it, balancing that with what value the vulnerability might provide to U.S. intelligence agencies. (22 pages)
Department Releases Intake and Charging Policy for Computer Crime Matters	Department of Justice	October 25, 2016	"In the course of recent litigation, the department yesterday shared the policy under which we choose whether to bring charges under the Computer Fraud and Abuse Act. As set forth in the memorandum, prosecutors must consider a number of factors in order to ensure that charges are brought only in cases that serve a substantial federal interest."
Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats (Project Report)	GWU Center for Cyber & Homeland Security	October 2016	The report places the current cyber threat in its larger strategic context and then assesses the role of private-sector active defense in addressing such threats. With this in mind, the report proposes a framework that defines the most prevalent active defense measures and places them along a spectrum of relative risk and impact, indicating where close coordination with the government becomes necessary for responsible private action. (86 pages)
Brief History of Law Enforcement Hacking in the United States	New America Foundation	September 2016	Understanding the history of government hacking is important in order to engage more people in the ongoing policy discussion. The paper focuses on a selection of illustrative historical cases, with the understanding that due to the secret nature of government investigations, only a fraction of the hacking that has taken place is known. This overview highlights major trends in investigative hacking and will hopefully foster more inquiries into these practices by policymakers and the public. (20 pages)
Predicting Cyber Attacks: A Study of the Successes and Failures of the Intelligence Community	Small Wars Journal	July 7, 2016	The article focuses on identifying the major successes and failures of analysis from the Intelligence Community (IC) to predict cyberattacks against the United States. The research goal is to break down the components of a good cyber defensive force into variables to clearly identify those failures and successes and their effects on the operational ability of the IC in cyberspace. (11 pages)
Tech for Jihad: Dissecting Jihadist's Digital Toolbox	Flashpoint	July 2016	The report attempts to catalog the 36 most noteworthy digital tools in common use by jihadists, and when they started using them. (13 pages)
Cyber Conflict: Prevention, Stability and Control	Carnegie Cyber Policy Initiative	July 2016	Only a few years ago, there were almost no norms globally accepted by governments on cybersecurity or cyber conflict. Even the United States, which had long pushed such

			norms, had publicly announced very few. The United States and a few other allies confirmed that laws of armed conflict (otherwise known as International Humanitarian Law or the "Geneva Convention") applied to cyberspace. Recently, this has changed with tremendous progress, so much so that 2015 was called the Year of Global Cyber Norms. (10 pages)
Combatting the Ransomware Blitzkrieg: The Only Defense is a Layered Defense, Layer One: Endpoint Security	The Institute for Critical Infrastructure Technology	April, 2016	The brief contains an analysis of the need for endpoint security; vulnerable endpoints (users, personal computers, servers, mobile devices, specialize hardware, and cloud services); potentially vulnerable endpoints (SCADA/ICS, IoT devices, cars); endpoint security; and selecting an endpoint security strategy. (27 pages)
Know Your Enemies 2.0: The Encyclopedia of the Most Prominent Hactivists, Nation State, and Mercenary Hackers	*Information for Critical Infrastructure Technologies (ICIT)*	February 2016	The report covers threat groups not by use of a particular ranking system, but by the dominant players categorized by geography. Zero days, malware, tool kits, exploit techniques, digital foot prints, and targets are covered in this encyclopedia. (81 pages)
Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study	*South Carolina Law Review*	January 12, 2016	"Although much work has been done on applying the law of warfare to cyberattacks, far less attention has been paid to defining a law of cyber peace applicable below the armed attack threshold. Among the most important unanswered questions is what exactly nations' due diligence obligations are to one another and to the private sector, as well as how these obligations should be translated into policy. In this article, we analyze how both the United States and the European Union are operationalizing the concept of cybersecurity due diligence, and then move on to investigate a menu of options presented to the European Parliament in November 2015 by the authors to further refine and apply this concept." (28 pages)
ISIS's OPSEC Manual Reveals How It Handles Cybersecurity	*Wired*	November 19, 2015	From the article, "So what exactly are ISIS attackers doing for OPSEC? It turns out ISIS has a 34-page guide to operational security, which offers some clues. [R]esearchers with the Combating Terrorism Center at West Point's military academy uncovered the manual and other related documents from ISIS forums and chat rooms."
2015 Annual Report to Congress	U.S.-China Economic Commission	November 17, 2015	Reportedly China causes increasing harm to the U.S. economy and security through two deliberate policies targeting the United States: (1) coordinated, government-backed theft of information from a wide variety of U.S.-based commercial enterprises and (2) widespread restrictions on content,

			standards, and commercial opportunities for U.S. businesses. Hackers working for the Chinese government—or with the government's support and encouragement—have infiltrated the computer networks of U.S. government agencies, contractors, and private companies, and stolen personal information and trade secrets. (See Chapter 1, Section 4: Commercial Cyber Espionage and Barriers to Digital Trade in China.) (631 pages)
Cyber Defense: An International View	U.S. Army War College Strategic Studies Institute	September 2015	The paper provides an overview of four different national approaches to cyber defense: those of Norway, Estonia, Germany, and Sweden. It also provides a guide for engaging with the relevant governmental and other organizations in each of these countries and compares and contrasts the advantages and drawbacks of each national approach. (65 pages)
Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box	Woodrow Wilson International Center for Scholars	August 1, 2015	"This policy brief outlines what the Deep Web and Darknet are, how they are accessed, and why we should care about them. For policymakers, the continuing growth of the Deep Web in general and the accelerated expansion of the Darknet in particular pose new policy challenges. The response to these challenges may have profound implications for civil liberties, national security, and the global economy." (20 pages)
Cyber-Enabled Economic Warfare: An Evolving Challenge	Hudson Institute	August 2015	This monograph is divided into six chapters: one dissecting the U.S.'s use of cyber-enabled economic warfare; two providing analyses of cyber-enabled economic warfare threats posed to the United States by state and non-state actors; two offering case studies of emerging cyber-enabled economic warfare in two key sectors, financial services and critical infrastructure; and a concluding chapter that reviews key takeaways and next steps. (174 pages)
Russian Underground 2.0	Trend Micro (Forward Looking Threat Team)	July 28, 2015	The Russian underground is a mature ecosystem that covers all aspects of cybercriminal business activities and offers an increasingly professional underground infrastructure for the sale of malicious goods and services. There is increasing professionalization of the crime business that allows cheaper prices to dominate sales and thereby make it easy and very affordable for anyone without significant skill to buy whatever is needed to conduct criminal dealings. (41 pages)
Below the Surface: Exploring the Deep Web	Trend Micro	June 22, 2015	The research paper offers a look into the duality of the Deep Web—how its ability to

			protect anonymity can be used to communicate freely, away from censorship and law enforcement, or be used to expedite dubious or criminal pursuits. It also briefly touches on the Deep Web's impact, and offers a forecast on how it could evolve over the next few years. (48 pages)
Cybersecurity: Jihadism and the Internet	European Parliament Think Tank	May 18, 2015	"Since the beginning of the conflict in Syria in March 2011, the numbers of European citizens supporting or joining the ranks of ISIL/Da'esh have been growing steadily, and may now be as high as 4,000 individuals. At the same time, the possible avenues for radicalisation are multiplying and the risks of domestic terrorism increasing. The proliferation of global jihadi messaging online and their reliance on social networks suggest that the Internet is increasingly a tool for promoting jihadist ideology, collecting funds, and mobilizing their ranks." (2 pages)
APT30 and the Mechanics of a Long-Running Cyber-Espionage Operation: How a Cyber Threat Group Exploited Governments and Commercial Entities Across Southeast Asia and India for Over a Decade	FireEye	April 2015	Reportedly a Chinese government hacking team has used the same basic set of tools to spy on Southeast Asian and Indian dignitaries for a decade, demonstrating the low level of cyber defenses protecting government information across broad swaths of the world. According to Fireeye, the fact this group, APT30, has been able to use the same basic set of malware tools against government networks since at least 2005 suggests its targets remained unaware for more than a decade they were being spied on or were incapable of countering the threat. (70 pages)
Worldwide Threat Assessment of the U.S. Intelligence Community	Director of National Intelligence	February 26, 2015	Cybersecurity is the first threat listed in this annual review of worldwide threats to the United States. Despite ever-improving network defenses, the diverse possibilities for remote hacking intrusions, supply chain operations to insert compromised hardware or software, and malevolent activities by human insiders will hold nearly all ICT systems at risk for years to come. Moreover, the risk calculus employed by some private-sector entities reportedly does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors. (29 pages)
The Impact of the Dark Web on Internet Governance and Cyber Security	Global Commission on Internet Governance	February 2015	The dark Web is a part of the deep Web that has been intentionally hidden and is inaccessible through standard web browsers. The deep Web has the potential to host an increasingly high number of malicious services and activities. To formulate comprehensive strategies and policies for governing the Internet, it is important to

			consider insights on its farthest reaches—the deep Web and, more importantly, the dark Web. The paper attempts to provide a broader understanding of the dark Web and its impact on people's lives. (18 pages)
Attributing Cyber Attacks	Thomas Rid and Ben Buchanan, *Journal of Strategic Studies*	December 23, 2014	The authors introduce the Q Model; designed to explain, guide, and improve the making of attribution. Matching an offender to an offence is an exercise in minimizing uncertainty on three levels: (1) tactically, attribution is an art as well as a science; (2) operationally, attribution is a nuanced process, not a black-and-white problem; and (3) strategically, attribution is a function of what is at stake politically. Successful attribution requires a range of skills on all levels, careful management, time, leadership, stress-testing, prudent communication, and recognizing limitations and challenges. (36 pages)
Operation Cleaver	Cylance	December 2, 2014	A sophisticated hacking group with ties to Iran has probed and infiltrated targets across the United States and 15 other nations during the past two years in a series of cyberattacks dubbed "Operation Cleaver." The Cleaver group has evolved faster than any previous Iranian campaign, according to the report, which calls Iran "the new China" and expresses concern that the group's surveillance operations could evolve into sophisticated, destructive attacks. (86 pages)
Legal Issues Related to Cyber	*NATO Legal Gazette*	December 2014	The *NATO Legal Gazette* contains thematically organized articles usually written by military or civilian legal personnel working at NATO or in the governments of NATO and partner nations. Its purpose is to share articles of significance for the large NATO legal community and connect legal professionals of the Alliance. It is not a formal NATO document. (74 pages)
The National Intelligence Strategy of the United States of America 2014	Office of the Director of National Intelligence	September 18, 2014	Cyber intelligence is one of four "primary topical missions" the intelligence community must accomplish. Both state and nonstate actors use digital technologies to achieve goals, such as fomenting instability or achieving economic and military advantages. They do so "often faster than our ability to understand the security implications and mitigate potential risks." To become more effective in the cyber arena, the intelligence community reportedly must improve its ability to correctly attribute attacks. (24 pages)
Today's Rising Terrorist Threat and the Danger to the United States: Reflections on	The Annenberg Public Policy Center	July 22, 2014	Members of the panel that studied the 2001 attacks urge Congress to enact cybersecurity

the Tenth Anniversary of the 9/11 Commission Report	and the Bipartisan Policy Center		legislation, the White House to communicate the consequences of potential cyberattacks to Americans, and leaders to work with allies to define what constitutes an online attack on another country. (48 pages)
Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies	Center for a New American Security	July 2014	The report examines existing information on technology security weaknesses and provides nine specific recommendations for the U.S. government and others to cope with these insecurities. (64 pages)
M Trends: Beyond the Breach: 2014 Threat Report	Mandiant	April 2014	Cyber-threat actors are expanding the uses of computer network exploitation to fulfill an array of objectives, from the economic to the political. Threat actors are not only interested in seizing the corporate "crown jewels" but are also looking for ways to publicize their views, cause physical destruction, and influence global decisionmakers. Private organizations have increasingly become collateral damage in political conflicts. Reportedly with no diplomatic solution in sight, the ability to detect and respond to attacks has never been more important. (28 pages)
Emerging Cyber Threats Report 2014	Georgia Institute of Technology	January 2014	Brief compilation of academic research on losing control of cloud data, insecure but connected devices, attackers adapting to mobile ecosystems, the high costs of defending against cyberattacks, and advances in information manipulation. (16 pages)
Cybersecurity and Cyberwar: What Everyone Needs to Know	Brookings Institution	January 2014	Authors Peter W. Singer and Allan Friedman look at cybersecurity issues faced by the military, government, businesses, and individuals and examine what happens when these entities try to balance security with freedom of speech and the ideals of an open Internet. (306 pages)
W32.Duqu: The Precursor to the Next Stuxnet	Symantec	November 14, 2013	On October 14, 2011, a research lab with strong international connections alerted Symantec to a sample that appeared to be very similar to Stuxnet, the malware that wreaked havoc in Iran's nuclear centrifuge farms. The lab named the threat *Duqu* because it creates files with the file name prefix *DQ*. The research lab provided Symantec with samples recovered from computer systems located in Europe as well as a detailed report with initial findings, including analysis comparing the threat to Stuxnet.
To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve	The Langner Group	November 2013	The report summarizes the most comprehensive research on the Stuxnet malware so far. It combines results from

			reverse engineering the attack code with intelligence on the design of the attacked plant and background information on the attacked uranium enrichment process. It looks at the attack vectors of the two different payloads contained in the malware and provides an analysis of the bigger and much more complex payload that was designed to damage centrifuge rotors by overpressure. (36 pages)
Strategies for Resolving the Cyber Attribution Challenge	Air University, Maxwell Air Force Base	May 2013	Private-sector reports have proven that it is possible to determine the geographic reference of threat actors to varying degrees. Based on these assumptions, nation-states, rather than individuals, should be held culpable for the malicious actions and other cyber threats that originate in or transit information systems within their borders or that are owned by their registered corporate entities. The work builds on other appealing arguments for state responsibility in cyberspace. (109 pages)
Role of Counterterrorism Law in Shaping 'ad Bellum' Norms for Cyber Warfare	International Law Studies (U.S. Naval War College)	April 1, 2013	"To date there has been little attention given to the possibility that international law generally and counterterrorism law in particular could and should develop a subset of cyber-counterterrorism law to respond to the inevitability of cyberattacks by terrorists and the use of cyber weapons by governments against terrorists, and to supplement existing international law governing cyber war where the intrusions do not meet the traditional kinetic thresholds." (42 pages)
The Tallinn Manual on the International Law Applicable to Cyber Warfare	Cambridge University Press/ NATO Cooperative Cyber Defence Center of Excellence	March 5, 2013	The Tallinn Manual identifies the international law applicable to cyber warfare and sets out 95 "black-letter rules" governing such conflicts. An extensive commentary accompanies each rule, which sets forth the rule's basis in treaty and customary law, explains how the group of experts interpreted applicable norms in the cyber context, and outlines any disagreements within the group as to the rule's application. (Note: The manual is not an official NATO publication but rather an expression of opinions of a group of independent experts acting solely in their personal capacities.) (302 pages)
Cyberterrorism: A Survey of Researchers	Swansea University	March 2013	The report provides an overview of findings from a project designed to capture current understandings of cyberterrorism within the research community. The project ran between June 2012 and November 2012, and it employed a questionnaire that was distributed to more than 600 researchers, authors, and other experts. A total of 118 responses were received from individuals

			working in 24 countries across six continents. (21 pages)
National Level Exercise 2012: Quick Look Report	Federal Emergency Management Agency (FEMA)	March 2013	National Level Exercise (NLE) 2012 was a series of exercise events that examined the ability of the United States to execute a coordinated response to a series of significant cyber incidents. The NLE 2012 series focused on examining four major themes: planning and implementation of the draft National Cyber Incident Response Plan (NCIRP), coordination among governmental entities, information sharing, and decision making. (22 pages)
Responding to Cyber Attacks and the Applicability of Existing International Law	Army War College	January 2013	The paper identifies how the United States should respond to the threat of cyber operations against essential government and private networks. First, it examines the applicability of established international law to cyber operations. Next, it proposes a method for categorizing cyber operations across a spectrum synchronized with established international law. Then, it discusses actions already taken by the United States to protect critical government and private networks and concludes with additional steps the United States should take to respond to the threat of cyber operations. (34 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)
Cyberattacks Among Rivals: 2001-2011 (from the article, "The Fog of Cyberwar" by Brandon Variano and Ryan Maness	*Foreign Affairs*	November 21, 2012	A chart showing cyberattacks by initiator and victim, 2001-2011. (Subscription required.)
Proactive Defense for Evolving Cyber Threats	Sandia National Labs	November 2012	The project applied rigorous predictability-based analytics to two central and complementary aspects of the network defense problem—attack strategies of the adversaries and vulnerabilities of the defenders' systems—and used the results to develop a scientifically grounded, practically implementable methodology for designing proactive cyber defense systems. (98 pages)

Safeguarding Cyber-Security, Fighting in Cyberspace	International Relations and Security Network (ISN)	October 22, 2012	Looks at the militarization of cybersecurity as a source of global tension and makes the case that cyber warfare is already an essential feature of many leading states' strategic calculations, followed by its opposite (i.e., the case that the threat posed by cyber warfare capabilities is woefully overstated).
Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World	Symantec Research Labs	October 16, 2012	The paper describes a method for automatically identifying zero-day attacks from field-gathered data that records when benign and malicious binaries are downloaded on 11 million real hosts around the world. Searching this data set for malicious files that exploit known vulnerabilities indicates which files appeared on the Internet before the corresponding vulnerabilities were disclosed. (12 pages)
Federal Support for and Involvement in State and Local Fusion Centers	Senate Permanent Subcommittee on Investigations	October 3, 2012	A two-year bipartisan investigation found that U.S. Department of Homeland Security efforts to engage state and local intelligence "fusion centers" have 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 November 10, 2011 Russian "cyberattack" in Illinois. (141 pages)
Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States	*First Monday*	July 2, 2012	The essay argues that current contradictory tendencies within U.S. cyber war discourse are unproductive and even potentially dangerous. It argues that the war metaphor and nuclear deterrence analogy are neither natural nor inevitable and that abandoning them would open up new possibilities for thinking more productively about the full spectrum of cybersecurity challenges, including the as-yet unrealized possibility of cyberwar.
Nodes and Codes: The Reality of Cyber Warfare	U.S. Army School of Advanced Military Studies, Command and General Staff	May 17, 2012	Explores the reality of cyber warfare through the story of Stuxnet. Three case studies evaluate cyber policy, discourse, and procurement in the United States, Russia, and China before and after Stuxnet to illustrate their similar, yet unique, realities of cyber warfare. (62 pages)
United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?	Triangle Institute for Security Studies	March 2012	The incongruence between national counterterrorism (CT) cyber policy, law, and strategy degrades the abilities of federal CT professionals to interdict transnational terrorists from within cyberspace. To optimize national CT assets and to stymie

			the growing threat posed by terrorists' ever-expanding use of cyberspace, national decision-makers should modify current policies to efficiently execute national CT strategies, albeit within the framework of existing CT cyber-related statutes. (34 pages)
A Cyberworm that Knows No Boundaries	RAND Corporation	December 21, 2011	Stuxnet-like worms pose a serious threat even to infrastructure and computer systems that are not connected to the Internet. Defending against such attacks is an increasingly complex prospect. (55 pages)
Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934	DOD	November 2011	"When warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means - diplomatic, informational, military< and economic - to defend our nation, our allies, our partners and our interests." (14 pages)
Cyber War Will Not Take Place	*Journal of Strategic Studies*	October 5, 2011	The paper argues that cyber warfare has never taken place, is not currently taking place, and is unlikely to take place in the future. (29 pages)
Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011	Office of the National Counterintelligence Executive	October 2011	Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment. (31 pages)
A Four-Day Dive Into Stuxnet's Heart	*Threat Level* Blog *(Wired)*	December 27, 2010	"It is a mark of the extreme oddity of the Stuxnet computer worm that Microsoft's Windows vulnerability team learned of it first from an obscure Belarusian security company that even they had never heard of."
Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? A Preliminary Assessment	Institute for Science and International Security	December 22, 2010	The report indicates that commands in the Stuxnet code intended to increase the frequency of devices targeted by the malware exactly match several frequencies at which rotors in centrifuges at Iran's Natanz enrichment plant are designed to operate optimally or are at risk of breaking down and flying apart. (10 pages)
Stuxnet Analysis	European Network and Information Security Agency	October 7, 2010	A European Union cybersecurity agency warns that the Stuxnet malware is a game changer for critical information infrastructure protection. Computer systems that monitor supervisory-controlled and data acquisition systems infected with the worm

			might be programmed to establish destructive over or under pressure conditions by running industrial pumps at different frequencies.
Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy	National Research Council	October 5, 2010	Per request of the Office of the Director of National Intelligence, the National Research Council undertook a two-phase project aimed to foster a broad, multidisciplinary examination of strategies for deterring cyberattacks on the United States and of the possible utility of these strategies for the U.S. government. (400 pages)
Cyber Warfare: Armageddon in a Teacup?	Army Command and General Staff, Fort Leavenworth	December 11, 2009	This study examines cyber warfare conducted against Estonia in 2007, Georgia in 2008, and Israel in 2008. According to the report, "In all three cases cyber warfare did not achieve strategic political objectives on its own. Cyber warfare employed in the three cases consisted mainly of Denial of Service attacks and website defacement. These attacks were a significant inconvenience to the affected nations, but the attacks were not of sufficient scope, sophistication, or duration to force a concession from the targeted nation. Cyber warfare offensive capability does not outmatch defensive capability to the extent that would allow the achievement of a strategic political objective through cyber warfare alone. The possibility of strategic-level cyber warfare remains great, but the capability has not been demonstrated at this time." (106 pages)

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are for documents; other cited resources are webpages.

Table 3. Cloud Computing,[2] "The Internet of Things,"[3] Smart Cities, and FedRAMP[4]

Title	Source	Date	Notes
About FedRAMP	FedRAMP.gov	Continuously Updated	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Internet of Things Consortium	Internet of Things Consortium	Continuously Updated	IoTC is comprised of hardware, software and analytics companies, in areas including home automation, wearables, connected cars, smart cities, 3D printing, and virtual/augmented reality. On behalf of its members, the IoTC is dedicated to the growth of the internet of things marketplace and the development of

			sustainable business models. The IoTC educates technology firms, retailers, insurance companies, marketers, media companies and the wider business community about the value of IoT.
Cyber-Physical Systems	National Science Foundation (NSF)	Continuously Updated	Cyber-physical systems (CPS) integrate sensing, computation, control, and networking into physical objects and infrastructure, connecting them to the Internet and to each other.
Cyber-Physical Systems	Office of Science and Technology Policy (OSTP), Networking and Information Technology Research and Development (NITRD) Program)	Continuously Updated	The CPS Senior Steering Group (SSG) is to coordinate programs, budgets, and policy recommendations for CPS research and development (R&D), which includes identifying and integrating requirements, conducting joint program planning, and developing joint strategies.
Cyber-Physical Systems	University of California, Berkeley	Continuously Updated	"CPS are integrations of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa."
Internet of Things Consortium	Technology hardware, software and analytics companies	Continuously Updated	IoTC is composed of hardware, software and analytics companies, in areas including home automation, wearables, connected cars, smart cities, 3D printing, and virtual/augmented reality. On behalf of its members, the IoTC is dedicated to the growth of the Internet of things marketplace and the development of sustainable business models. The IoTC educates technology firms, retailers, insurance companies, marketers, media companies, and the wider business community about the value of IoT.
Newly Launched 'Trusted IoT Alliance' Unites the Industry to Further a Blockchain-based Internet of Things	Medium	September 19, 2017	The mission of the Trusted IoT Alliance is to bring companies together to develop and set the standard for an open source blockchain protocol to support IoT technology in major industries worldwide. The Alliance plans to fund small grants to support open source development and is reviewing proposals from IoT and blockchain technologists.

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD	GAO	July 27, 2017	Congress included provisions in reports associated with two separate statutes for GAO to assess the IoT-associated security challenges faced by DOD. This report (1) addresses the extent to which DOD has identified and assessed security risks related to IoT devices, (2) assesses the extent to which DOD has developed policies and guidance related to IoT devices, and (3) describes other actions DOD has taken to address security risks related to IoT devices.(46 pages)
Internet of Things: Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise	GAO	July 26, 2017	All four of the communities that GAO reviewed are using federal funds in combination with other resources, both financial and non-financial, to plan and deploy IoT projects. For example, one community used the $40 million DOT award to leverage, from community partners, more than $100 million in additional direct and in-kind contributions, such as research or equipment contributions. Communities discussed four main challenges to deploying IoT, including community sectors (e.g., transportation, energy, and public safety) that are siloed and proprietary systems that are not interoperable with one another. (45 pages)
The Internet of Things Connectivity Binge: What Are the Implications?	Pew Research Center	June 6, 2017	As automobiles, medical devices, smart TVs, manufacturing equipment and other tools and infrastructure are networked, is it likely that attacks, hacks or ransomware concerns in the next decade will cause significant numbers of people to decide to disconnect, or will the trend toward greater connectivity of objects and people continue unabated? Some 1,201 responded to this nonscientific canvassing: 15% of these particular respondents said significant numbers would disconnect and 85% chose the option that most people will move more deeply into connected life. (94 pages)
Technology Assessment: Internet of Things: Status and implications of an increasingly connected world	GAO	May 15, 2017	GAO reviewed key reports and scientific literature; convened two expert meetings with the assistance of the National Academies; and interviewed officials from two agencies to obtain their views on specific implications of the IoT. (78 pages)

IoT, Automation, Autonomy, and Megacities in 2025	Center for Strategic & International Studies	April 26, 2017	Engineers designing and implementing internet-connected IOT devices face daunting challenges that is creating a discomfort with what they see evolving in their infrastructures. This paper brings their concerns to life by extrapolating from present trends to describe plausible (likely?) future crises playing out in multiple global cities within 10 years. Much of what occurs in the scenarios is fully possible today. This paper attempts to reveal what is possible when these technologies are applied to critical infrastructure applications en masse without adequate security in densely populated cities of the near future that are less resilient than other environments. (16 pages)
The Cyber Shield Act: Is the Legislative Community Finally Listening to Cybersecurity Experts?	Institute for Critical Infrastructure Technology	April 2017	There are three main criteria to ensure a Cyber Shield program works. First, officials must ensure industry leaders are involved in developing the ratings but not leading the team. Second, the program should include a substantial public education component aimed at making consumers care enough about cybersecurity that the rankings actually change their buying decisions. Finally, the rankings themselves should go beyond a mere one-star to five-star ranking to incorporate more dynamic data. (8 pages)
A 21st Century Cyber-Physical Systems Education	National Academy of Sciences Computer Science and Telecommunications Board	February 2017	The report describes the knowledge and skills required to engineer increasingly capable, adaptable, and trustworthy systems that integrate the cyber and physical worlds and recommends paths for creating the courses and programs needed to educate the engineering workforce that builds them. (107 pages)
A Data Privacy Playbook	Berkman Klein Center (Harvard)	February 2017	Opening data has many important benefits, but sharing data comes with inherent risks to individual privacy: released data can reveal information about individuals that would otherwise not be public knowledge. The document is takes a first step toward codifying responsible privacy-protective approaches and processes that could be adopted by cities and other groups that are publicly releasing data. (111 pages)
Cross-Device Tracking: An FTC Staff	FTC	January 23,	The report describes the technology

Report		2017	used to track consumers across multiple Internet-connected devices, the benefits and challenges associated with it, and industry efforts to address those challenges. The report concludes by making recommendations to industry about how to apply traditional principles like transparency, choice, and security to this relatively new practice. (23 pages)
Rise of the Machines: the Dyn Attack Was Just a Practice Run	Institute for Critical Infrastructure Technology	December 2016	The Mirai IoT botnet has inspired a renaissance in adversarial interest in DDoS botnet innovation based on the lack of fundamental security-by-design in the Internet and in IoT devices... The report provides a comprehensive and detailed analysis of this threat which has forced stakeholders to recognize the lack of security by design and the prevalence of vulnerabilities inherent in the foundational design of IoT devices. (62 pages)
Internet of Things will demand a step-change in search solutions	IEEE Intelligent Systems	November 23, 2016	With more and more IoT devices being connected to the Internet, and smart city data projects starting to be implemented, there is an urgent need to develop new search solutions that will allow information from IoT sources to be found and extracted. Although existing search engines have ever more sophisticated and effective ways of crawling through web pages and searching for textual data, the article argues that they will not be effective in accessing the type of numerical and sensory data that IoT devices will need to gather. (5 pages)
Internet of Things (IoT) Security and Privacy Recommendations	Broadband Internet Technical Advisory Group (BITAG)	November 22, 2017	BITAG believes the recommendations outlined in this report may help to dramatically improve the security and privacy of IoT devices and minimize the costs associated with collateral damage. In addition, unless the IoT device sector —the sector of the industry that manufactures and distributes these devices—improves device security and privacy, consumer backlash may impede the growth of the IoT marketplace and ultimately limit the promise that IoT holds. (43 pages)
Strategic Principles for Securing the Internet of Things	DHS	November 15, 2016	The document explains IoT risks and provides a set of non-binding principles and suggested best practices to build toward a

			responsible level of security for the devices and systems businesses design, manufacture, own, and operate. (17 pages)
Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	NIST	November 2016	NIST formally unveiled their guidelines for increasing the security of Internet-connected devices. The guide provides security guidelines for 30 different processes involved with managing Internet-connected devices, from the supply phase to testing. (257 pages)
Building Smart Communities for the Future: Proceedings of a Workshop	National Academies Press	October 2016	Summary of presentations at June 21-22, 2016, Government-University-Industry Research Roundtable (GUIRR) meeting to explore the role of connectedness and sustainability in developing smart communities; the challenges and opportunities associated with the roll-out of intelligent systems; and the partnerships among governments, universities, and industry that are integral to these advances. (8 pages)
Announcing Over $80 million in New Federal Investment and a 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 over $80 million in new federal investments and a doubling of the number of participating cities and communities, exceeding 70 in total.
Demystifying the Internet of Things	(Information Technology Laboratory) ITL Bulletin	September 2016	NIST SP800-183 offers an underlying and foundational science for IoT—based technologies on the realization that IoT involves sensing, computing, communication, and actuation. It presents a common vocabulary to foster a better understanding of IoT and better communication between those parties discussing IoT. (4 pages)
Increasing the Potential of IoT through Security and Transparency	NTIA	August 2, 2016	NTIA is planning to launch a new multistakeholder process to support better consumer understanding of IoT products that support security upgrades. They have used this approach to help make progress on

			issues such as cybersecurity vulnerability disclosure and to provide more transparency about data collected by mobile apps. Given the burgeoning consumer adoption of IoT, the time seems ripe to bring stakeholders together to help drive some guidelines to encourage the growth of IoT.
Network of 'Things'	NIST	July 28, 2016	The publication provides a basic model aimed at helping researchers better understand IoT and its security challenges. (30 pages)
How Is the Federal Government Using the Internet of Things?	Center for Data Innovation	July 25, 2016	The federal government faces a number of challenges that have slowed the adoption of IoT in the public sector. First, there is a lack of strategic leadership at the federal level about how to make use of IoT. Second, federal agencies do not always have workers with the necessary technical skills to effectively use data generated by IoT. Third, federal agencies do not have sufficient funding to modernize their IT infrastructure and begin implementing IoT pilot projects. Fourth, even when funding exists, federal procurement policies often make it difficult for agencies to quickly and easily adopt the technology. Finally, risks and uncertainty—about privacy, security, interoperability, and return on investment—delay federal adoption as potential federal users wait for the technology to mature and others to adopt first. (30 pages)
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	FTC Bureau of Consumer Protection and Office of Policy Planning	June 2, 2016	FTC staff comment on NTIA's Request for Comment on the Internet of Things. The comment highlights lessons learned from the FTC's law enforcement, consumer and business education, and policy activities relating to these issues. It then addresses the benefits and risks of IoT, highlights some best practice recommendations for industry, discusses the role of government in fostering innovation in IoT products and services, and sets forth some considerations for NTIA in setting standards and promoting interoperability. (17 pages)
Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance	GAO	April 7, 2016	GAO was asked to examine federal agencies' use of Service Level Agreements (SLAs). GAO's objectives were to (1) identify key

			practices in cloud computing SLAs and (2) determine the extent to which federal agencies have incorporated such practices into their SLAs. GAO analyzed research, studies, and guidance developed by federal and private entities to establish a list of key practices to be included in SLAs. GAO validated its list with the entities, including OMB, and analyzed 21 cloud service contracts and related documents of five agencies (with the largest fiscal year 2015 IT budgets) against the key practices to identify any variances, their causes, and impacts. (46 pages)
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	National Telecommunications and Information Administration (NTIA)	April 6, 2016	NTIA is initiating an inquiry regarding the Internet of Things (IoT) to review the current technological and policy landscape. Through this notice, NTIA seeks broad input from all interested stakeholders—including the private industry, researchers, academia, and civil society—on the potential benefits and challenges of these technologies and what role, if any, the U.S. government should play in this area. After analyzing the comments, the department intends to issue a "green paper" that identifies key issues impacting deployment of these technologies, highlights potential benefits and challenges, and identifies possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector. (5 pages)
Product Testing and Validation	Underwriters Laboratories	April 4, 2016	The UL Cybersecurity Assurance Program (CAP) certification verifies that a product offers a reasonable level of protection against threats that may result in unintended or unauthorized access, change or disruption.... The [UL 2900] Standard contains requirements for the vendor to design the security controls in such a way that they demonstrably satisfy the security needs of the product. The Standard also describes testing and verification requirements aimed at collecting evidence that the designed security controls are implemented.
Alternative perspectives on the Internet of Things	Brookings Institution	March 25, 2016	Brookings scholars contribute their individual perspectives on the policy challenges and opportunities associated with IoT.

Emerging Cyber Threats Report 2016	Georgia Institute of Technology Cybersecurity Summit 2015	November 2015	"The intersection of the physical and digital world continued to deepen in 2015. The adoption of network-connected devices and sensors—the Internet of Things—accelerated and was expected to reach nearly 5 billion devices by the end of the year." (20 pages)
Interim Report on 21st Century Cyber-Physical Systems Education	NSF	July 2015	"CPS [also known as The Internet of Things] are increasingly relied on to provide the functionality and value to products, systems, and infrastructure in sectors including transportation, health care, manufacturing, and electrical power generation and distribution. CPS are smart, networked systems with embedded sensors, computer processors, and actuators that sense and interact with the physical world; support real-time, guaranteed performance; and are often found in critical applications." (48 pages)
Internet of Things: Mapping the Value Beyond the Hype	McKinsey Global Institute	June 2015	The paper is based upon a study of more than 100 use cases of the Internet of Things' (IoT's) potential economic impact within next 10 years. It outlines who will benefit and by how much. It also covers the factors—both enablers and barriers—that organizations face as they develop their IoT solutions. (144 pages)
Cloud Computing: Should Companies Do Most of Their Computing in the Cloud?	*The Economist*	May 26, 2015	Big companies have embraced the cloud more slowly than expected. Some are holding back because of costs and others are wary of entrusting sensitive data to another firm's servers. Should companies be doing most of their computing in the cloud? Representing the "Yes" viewpoint is Simon Crosby, co-founder and chief technology officer (CTO) of Bromium Inc. Representing the "No" viewpoint is Bruce Schneier, CTO at Resilient Systems.
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 IoT. Like the former Mobile Technology Unit (MTU), the new

			office will be housed in the Bureau of Consumer Protection and is the agency's latest effort to ensure that its core consumer protection mission keeps pace with the rapidly evolving digital economy. Kristin Cohen, the current chief of the MTU, will lead the work of the OTRI.
Insecurity in the Internet of Things (IoT)	Symantec	March 12, 2015	Symantec analyzed 50 smart home devices available today and found that none of them enforced strong passwords, used mutual authentication, or protected accounts against brute-force attacks. Of the mobile apps used to control the tested IoT devices, almost two out of 10 did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The tested IoT technology also contained many common vulnerabilities. (20 pages)
FedRAMP High Baseline	General Services Administration (GSA)	February 3, 2015	GSA released a draft of security-control requirements for cloud-computer systems purchased by federal agencies for "high-impact" uses. High-impact data will likely consist of health and law-enforcement data, but not classified information. Currently, cloud computing vendors seeking to sell to federal agencies must obtain security accreditation through FedRAMP. To date, FedRAMP has offered accreditations up to the moderate-impact level. About 80% of federal IT systems are low- and moderate-impacts.
What is The Internet of Things?	O'Reilly Media	January 2015	Ubiquitous connectivity is meeting the era of data. Since working with large quantities of data became dramatically cheaper and easier a few years ago, everything that touches software has become instrumented and optimized. Finance, advertising, retail, logistics, academia, and practically every other discipline has sought to measure, model, and tweak its way to efficiency. Software can ingest data from many inputs, interpret it, and then issue commands in real time. (Free registration required.) (32 pages)
FedRAMP Forward: 2 Year Priorities	General Services Administration (GSA)	December 17, 2014	The report addresses how the program will develop over the next two years. GSA is focusing on three goals for FedRAMP: • increased compliance and

			agency participation, • improved efficiencies, and • continued adaptation. (14 pages)
The Internet of Things: 2014 OECD Tech Insight Forum	Organisation for Economic Co-operation and Development (OECD)	December 11, 2014	The IoT extends Internet connectivity beyond traditional machines such as computers, smartphones, and tablets to a diverse range of every-day devices that use embedded technology to interact with the environment, all via the Internet. How can this collected data be used? What new opportunities will this create for employment and economic growth? How can societies benefit from technical developments to health, transport, safety and security, business, and public services? The OECD Technology Foresight Forum facilitated discussion on what policies and practices will enable or inhibit the ability of economies to seize the benefits of IoT.
DOD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process	Department of Defense (DOD) Inspector General	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)
NSTAC Report to the President on the Internet of Things	President's National Security Telecommunications Advisory Committee	November 18, 2014	The NSTAC unanimously approved a recommendation that governmental Internet traffic could get priority transmission during emergencies. The government already gets emergency priority in more traditional communications networks like the phone system through programs such as the Government Emergency Telecommunications Service (GETS). NSTAC now is proposing a GETS for the Internet. (56 pages)
The Department of Energy's Management of Cloud Computing Activities: Audit Report	Department of Energy (DOE) Inspector General	September 1, 2014	According to the inspector general, DOE should do a better job buying, implementing, and managing its cloud computing services. Programs and sites department-wide have independently spent more than $30 million on cloud services, but the chief information officer's office could not accurately account for the money. (20 pages)
Cloud Computing: The Concept,	Organization for	August 19,	The report gives an overview of

Impacts, and the Role of Government Policy	Economic Co-operation and Development (OECD)	2014	cloud computing, it • presents the concept, the services it provides, and deployment models; • discusses how cloud computing changes the way computing is carried out; • evaluates the impacts of cloud computing (including its benefits and challenges as well as its economic and environmental impacts); and • discusses the policy issues raised by cloud computing and the roles of governments and other stakeholders in addressing these issues. (240 pages)
Internet of Things: the Influence of M2M Data on the Energy Industry	GigaOm Research	March 4, 2014	The report examines the drivers of machine-2-machine (M2M)-data exploitation in the smart-grid sector and the oil and gas sector, as well as the risks and opportunities for buyers and suppliers of the related core technologies and services. (21 pages)
Software Defined Perimeter	Cloud Security Alliance	December 1, 2013	Cloud Security Alliance's software defined perimeter (SDP) initiative aims to make "invisible networks" accessible to a wider range of government agencies and corporations. The initiative will foster the development of architecture for securing the IoT using the cloud to create highly secure end-to-end networks between IP-addressable entities. (13 pages)
Delivering on the Promise of Big Data and the Cloud	Booz Allen Hamilton	January 9, 2013	Reference architecture does away with conventional data and analytics silos, consolidating all information into a single medium designed to foster connections called a 'data lake,' which reduces complexity and creates efficiencies that improve data visualization to allow for easier insights by analysts. (7 pages)
Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators	House Judiciary Committee, Subcommittee on Intellectual Property, Competition, and the Internet	July 25, 2012	Overview and discussion of cloud computing issues. (156 pages)
Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned	Government Accountability Office (GAO)	July 11, 2012	GAO recommends that the Secretaries of Agriculture, Health and Human Services, Homeland Security, State, and the Treasury, and

			the Administrators of the General Services Administration, and Small Business Administration 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, as applicable. (43 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 that is agile, secure, and cost-effective and to a service environment that can rapidly respond to changing mission needs. (44 pages)
A Global Reality: Governmental Access to Data in the Cloud—A Comparative Analysis of Ten International Jurisdictions	Hogan Lovells	May 23, 2012	The white paper compares the nature and extent of governmental access to data in the cloud in many jurisdictions around the world. (13 pages)
Policy Challenges of Cross-Border Cloud Computing	U.S. International Trade Commission	May 2012	The report examines the main policy challenges associated with cross-border cloud computing—data privacy, security, and ensuring the free flow of information—and the ways countries are addressing them through domestic policymaking, international agreements, and other cooperative arrangements. (38 pages)
Cloud Computing Synopsis and Recommendations (SP 800-146)	National Institute of Standards and Technology (NIST)	May 2012	NIST's guide explains cloud technologies in plain terms to federal agencies and provides recommendations for IT decisionmakers. (81 pages)
Global Cloud Computing Scorecard a Blueprint for Economic Opportunity	Business Software Alliance	February 2, 2012	The report notes that although many developed countries have adjusted their laws and regulations to address cloud computing, the wide differences in those rules make it difficult for companies to invest in the technology. (24 pages)
Concept of Operations: FedRAMP	General Services Administration (GSA)	February 7, 2012	FedRAMP is implemented in phases. The document describes all the services that were available at the 2012 initial operating capability. The concept of operations is updated as the program evolves toward sustained operations. (47 pages)
Federal Risk and Authorization	Federal Chief	January 4,	FedRAMP provides a standard

Management Program (FedRAMP)	Information Officers Council	2012	approach to assessing and authorizing (A&A) cloud computing services and products.
Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP)	White House/Office of Management and Budget (OMB)	December 8, 2011	FedRAMP is now required for all agencies purchasing storage, applications, and other remote services from vendors. The Administration promotes cloud computing as a means to save money and accelerate the government's adoption of new technologies. (7 pages)
U.S. Government Cloud Computing Technology Roadmap, Volume I, Release 1.0 (Draft). High-Priority Requirements to Further USG Agency Cloud Computing Adoption (SP 500-293)	National Institute of Standards and Technology (NIST)	December 1, 2011	Volume I is aimed at interested parties that wish to gain a general understanding and overview of the background, purpose, context, work, results, and next steps of the U.S. Government Cloud Computing Technology Roadmap initiative. (32 pages)
U.S. Government Cloud Computing Technology Roadmap, Volume II, Release 1.0 (Draft), Useful Information for Cloud Adopters (SP 500-293)	National Institute of Standards and Technology (NIST)	December 1, 2011	Volume II is designed as a technical reference for those actively working on strategic and tactical cloud computing initiatives including, but not limited to, U.S. government cloud adopters. This volume integrates and summarizes the work completed as of 2011 and explains how these findings support the roadmap introduced in Volume I. (85 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)
Cloud Computing Reference Architecture (SP 500-292)	NIST	September 1, 2011	The special publication, which is not an official U.S. government standard, is designed to provide guidance to specific communities of practitioners and researchers. (35 pages)
Federal Cloud Computing Strategy	White House	February 8, 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's goals are 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)
Federal Guidance Needed to Address Control Issues With Implementing Cloud Computing	GAO	July 1, 2010	The report suggests that the OMB director should establish milestones for completing a strategy for implementing the federal cloud computing initiative to assist federal agencies in identifying uses for and information security measures to use in implementing cloud computing. (53 pages)

Source: Highlights compiled by CRS from the reports.

Notes: Page counts are for documents; other cited resources are webpages.

Author Contact Information

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

Footnotes

1. "A breach constitutes a 'major incident' when it involves[personally identifiable information] that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people," the [OMB] memo states. "An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a 'major incident.'" Source: Fiscal Year 2016-2017 on Federal Information Security and Privacy Management Requirements, November 4, 2016.

2. Cloud computing is a web-based service that allows users to access anything from email to social media on a third-party computer. For example, Gmail and Yahoo are cloud-based email services that allow users to access and store emails that are saved on each respective service's computer, rather than on the individual's computer.

3. The "Internet of Things" (IoT) refers to networks of objects that communicate with other objects and with computers through the Internet. "Things" may include virtually any object for which remote communication, data collection, or control might be useful, such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems. See also CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer.

4. The Federal Risk and Authorization Management Program (FedRAMP) was established in December 2011 to provide a government-wide standard, centralized approach to assessing and authorizing cloud computing services and products. It reached initial operational capabilities in June 2012 and became fully operational during FY2014. See also CRS Report R42887, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, by Patricia Moloney Figliola and Eric A. Fischer.

CRS Reports & Analysis

Cybersecurity: Federal Government Authoritative Reports and Resources
November 13, 2017 (R44427)
Jump to Main Text of Report
Rita Tehan, Senior Research Librarian (rtehan@crs.loc.gov, 7-6739)

Related Author

- Rita Tehan

Contents

Tables

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 Rita Tehan
- CRS Report R44406, *Cybersecurity: Education, Training, and R&D Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44408, *Cybersecurity: Cybercrime and National Security Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44410, *Cybersecurity: Critical Infrastructure Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R44417, *Cybersecurity: State, Local, and International Authoritative Reports and Resources*, by Rita Tehan
- CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan
- CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan

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 Identities in Cyberspace (NSTIC)	National Institute of Standards and Technology (NIST)	Continuously Updated	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 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.
State of (US) Federal Information Technology Report	US CIO Council	January 19, 2017	The publication provides an overview of the government's path to the current state of information technology and 11 recommendations for the future of government information technology. (155 pages)
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

Report to the President on Federal IT Modernization - Request for Comment	American Technology Council	August 30, 2017	The ATC's plan first calls for the technical standards agency NIST to send OMB instructions for how to protect these high-value assets. Next, it directs OMB and the Department of Homeland Security (DHS) to produce a report about common vulnerabilities in these systems. Agencies with serious vulnerabilities would then have to submit a "remediation plan." (52 pages)
Information Technology: Opportunities for Improving Acquisitions and Operations	GAO	April 11, 2017	GAO assembled a panel of information technology (IT) experts on September 14, 2016, to elicit additional ideas to further improve delivery and operations of IT. Forum participants discussed the challenges and opportunities for chief information officers (CIO) to improve IT acquisitions and operations—with the goal of better informing policymakers and government leadership. They identified key actions related to the following topics: strengthening the Federal Information Technology Acquisition Reform Act (FITARA), improving CIO authorities, budget formulation, governance, workforce, operations, and transition planning. (32 pages)
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 General (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)
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 agencies—the Departments of Energy, Homeland Security, State, and Transportation; the Environmental Protection Agency; and the Office of Personnel Management—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)
Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information	DOD	November 18, 2013	The regulation imposed two new requirements: (1) an obligation 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 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 policy—Secure Hypertext Transfer Protocol (HTTPS) and the Digital Analytics Program (DAP).
Database of Unclassified Federal Cyber Spending	Taxpayers for Common Sense	Continuously Updated	The database presents information on unclassified federal cyber spending from FY2007 to FY2016. Dollar figures are actual numbers through 2015. FY2016 numbers are estimates included with President Obama's FY2017 budget request.
Oversight.gov	Council of the Inspectors General on Integrity and Efficiency (CIGIE)	Continuously Updated	The site includes a publicly accessible, text searchable repository of reports published by participating federal inspectors general (IGs). The reports appearing on Oversight.gov, as well as the data associated with them, have been posted directly to the site by the IG that issued it.
Information Security: OPM Has Improved Controls, but Further Efforts Are Needed	GAO	August 3, 2017	GAO evaluated OPM's (1) actions since the 2015 reported data breaches to prevent, mitigate, and respond to data breaches involving sensitive personnel records and information; (2) information security policies and practices for implementing selected government-wide initiatives and requirements; and (3) procedures for overseeing the security of OPM information maintained by contractors providing IT services. (42 pages)
State Department Telecommunications: Information on Vendors and Cyber-Threat Nations	GAO	July 27, 2017	Federal telecommunications systems can include a variety of equipment, products, and

			services that may be produced by foreign manufacturers—and may potentially be vulnerable to manipulation by a cyber-threat nation like China, Iran, North Korea, or Russia. GAO examined foreign manufacturers of the State Department's critical telecommunications equipment and services to identify those that might be closely linked to these nations. GAO did not identify any reported close link but did identify some manufacturers, software developers, and contractors that had suppliers that were based in one of these nations. (15 pages)
Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data	GAO	July 26, 2017	During FY2016, IRS made improvements in access controls over a number of system administrator accounts and updated certain software to prevent exposure to known vulnerabilities. However, the agency did not always (1) limit or prevent unnecessary access to systems, (2) monitor system activities to reasonably assure compliance with security policies, (3) reasonably assure that software was vendor supported and updated to protect against known vulnerabilities, (4) segregate incompatible duties, and (5) update system contingency plans to reflect changes to the operating environment. (42 pages)
Department of Veterans Affairs Federal Information Security Management Act (FISMA) Audit for FY 2016	Veterans Affairs Inspector General	June 21, 2017	The audit, noting some improvements, identified continuing significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems. Further, VA has not remediated approximately 7,200 outstanding system security risks in its corresponding Plans of Action and Milestones to improve its information security posture. (67 pages)
Semiannual Report to Congress, October 1, 2016 to March	Health and Human Services Dept. Inspector General	June 2, 2017	The amount and complexity of HHS data makes it difficult for the department to adequately protect that data from hackers and from improper access by employees and contractors. The report states that the department is conducting penetration testing of HHS networks and applications to determine whether security safeguards are strong enough. The tests also aim to determine how sophisticated an attacker would have to be to gain access to data and how likely the department is to spot the penetration. (77 pages)
Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed	GAO	May 18, 2017	GAO analyzed DHS's efforts to implement a sample of 31 of 109 action plans that DHS had reported as complete and that described later-stage implementation steps. To determine challenges, GAO analyzed and compared DHS documentation, including a random sample of IT-related contracts and agreements, to selected FITARA provisions to identify gaps between what was required by FITARA and what DHS had implemented. (58 pages)

Cybersecurity: Actions Needed to Strengthen U.S. Capabilities.	GAO	February 14, 2017	The statement (1) provides an overview of GAO's work related to cybersecurity of the federal government and the nation's critical infrastructure and (2) identifies areas of consistency between GAO recommendations and those recently made by the Cybersecurity Commission and CSIS. Over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of February 2017, about 1,000 recommendations had not been implemented. (25 pages)
Industrial Control System Security Within NASA's Critical and Supporting Infrastructure	NASA Office of Inspector General	February 8, 2017	The report examined "whether NASA has implemented effective policies, procedures, and controls to protect the systems it uses to operate its critical infrastructure." The report found that that agency "has not adequately defined OT, developed a centralized inventory of OT systems, or established a standard protocol to protect systems that contain OT components." Problems arise due to the complications inherent in combining manual operational technology systems with more sophisticated IT systems. For example, using IT security practices to address issues in IT systems can cause malfunctions. (30 pages)
Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016	HHS Office of Inspector General	February 2017	HHS is making progress in improving its information security practices, but it still has gaps that put sensitive data and systems at risk of compromise. The OIG report notes that overall, in comparison to its FISMA review of HHS a year ago, the agency has made improvements, with the number of negative findings declining. (69 pages)
Fifth Generation Wireless Network and Device Security	FCC	January 23, 2017	The FCCommission seeks comment on new security issues that implementation of the fifth generation (5G) wireless network and device security presents to the general public, and on the current state of planning to address these issues. The inquiry, focusing on cybersecurity for 5G, raises fundamental questions about scope and responsibilities for such security. The proceeding's goal is to begin a conversation on the state of 5G wireless network and device security and to foster a dialogue on the best methods for ensuring that the 5G wireless networks and devices used by service providers in their operations are secure from the beginning. (6 pages)
Cybersecurity Risk Reduction	FCC	January 18, 2017	The white paper describes the risk reduction portfolio of the current FCC and suggests actions to affirmatively reduce cyberrisk in a manner that incents competition, protects consumers, and reduces significant national security risks. The document presents a strategy to promote an acceptable balance between corporate and consumer interests in cyber risk management when elements of market failure are at work. It acknowledges that the commission's preference is to work collaboratively with industry using private and

			public partnerships. However, if market forces do not result in a tolerable risk outcome, the commission has tools available to make adjustments to restore the balance. (56 pages)
Designation of Election Infrastructure as a Critical Infrastructure Subsector	DHS	January 6, 2017	DHS has added the U.S. election infrastructure to the list of protected critical infrastructure sectors of the economy. This designation means that election infrastructure becomes a priority within the National Infrastructure Protection Plan. It also enables DHS to prioritize its cybersecurity assistance to state and local election officials, but only for those who request it.
Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and FDA Staff	FDA	December 28, 2016	The guidance informs industry and FDA staff of the agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices. In addition to the specific recommendations contained in the guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. (30 pages)
Cybersecurity Considerations for Benefit Plans	2016 ERISA Advisory Council (Department of Labor)	November 10, 2016	The ERISA Advisory Council offered its final suggestions on cybersecurity protections for retirement plans to the Department of Labor. The council boiled its recommendations down to two: make its report publicly available as soon as administratively feasible and provide information to the employee benefit plan community to educate them on cybersecurity risks and potential approaches for managing those risks. (33 pages)
Federal Information Security Modernization Act Audit FY 2016	OPM Inspector General	November 9, 2016	OPM still suffers from extensive cyber weaknesses, including inadequate scanning for computer vulnerabilities and extremely high turnover among staffers responsible for information security. The turnover also contributed to a "significant regression" in OPM compliance with FISMA. (94 pages)
Cybersecurity Incident Handling Is Ineffective and Incomplete	DOT Inspector General	October 13, 2016	The audit assessed DOT's policies and procedures for (1) monitoring, detecting, and eradicating cyber incidents, and (2) reporting incidents and their resolutions to appropriate authorities. DOT's Office of Chief Information Officer (OCIO) has not ensured that the Department's Security Operations Center has access to all departmental systems or required the center to consider incident risk, thus limiting the center's ability to effectively monitor, detect, and eradicate cyber incidents. (18 pages)
Commodity Futures Trading Commission's Policies and Procedures For Reviewing Registrants' Cybersecurity Policies	CFTC Inspector General	October 11, 2016	The audit found that the CFTC, in conducting cyber security examinations of the firms, did not employ a "risk-based approach" to "independently test results of the cybersecurity assessments" it prepared. The finding sparked sharp disagreement with the CFTC, which in a

			response to the audit defended its exams and disputed the way the watchdog characterized them. (49 pages)
Department of Energy's Unclassified Cybersecurity Program 2016	DOE Inspector General	October 2016	DOE has made progress shoring up vulnerabilities previously identified by its inspector general in unclassified IT systems, but significant flaws persist. The audit indicates "issues related to vulnerability management, system integrity of web applications, access controls and segregation of duties, and configuration management, continue to exist." The audit goes on to list several issues that call into question DOE's vulnerability management program. (25 pages)
Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community	DHS	October 2016	The framework is a resource to help critical infrastructure owners and operators, and other private sector, federal, and state, local, tribal, and territorial (SLTT) government partners that share threat information, learn where they can turn, and in what circumstances, to both receive and report threat information. Threat information in the framework is limited to information sharing pertaining to man-made threats, including both cyber and physical threats, to critical infrastructure. The document is not new policy, but describes the various processes and mechanisms currently used to share threat information and the existing array of threat information-sharing entities involved in those processes. (110 pages)
FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk	GAO	September 29, 2016	The FDA did not fully or consistently implement access 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)
Cybersecurity Act of 2015 Report: EPA's Policies and Procedures to Protect Systems With Personally Identifiable Information	EPA Office of Inspector General	August 11, 2016	OIG conducted an audit to determine to what extent the EPA implemented information system security policies and procedures to protect agency systems that provide access to national security or Personally Identifiable

			Information (PII), as outlined in Section 406 of the Cybersecurity Act of 2015. The report addresses EPA's goal or cross-agency strategy: Embracing EPA as a high-performing organization. (The full report is not public.) (1 page)
U.S. General Services Administration Cybersecurity Act Assessment	GSA Office of Inspector General	August 10, 2016	GSA policies and procedures regarding access controls are generally consistent with significant government-wide policies and procedures, including relevant standards established by NIST and OMB, according to GSA's Office of Inspector General. (9 pages)
Inspection of Federal Computer Security at the U.S. Department of the Interior	Dept. of Interior Office of Inspector General	August 9, 2016	DOI has implemented measures, such as multifactor authentication and software inventory management, to reduce the risk of unauthorized access to its computer systems and prevent spending public funds on unused software. DOI, however, needs to update its logical access controls to meet current standards, ensure that its mobile computing devices are encrypted and securely configured, and obtain the ability to inspect encrypted traffic for malicious content. (21 pages)
Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015	Department of Commerce	August 4, 2016	Commerce's logical access policies generally followed appropriate standards and specific operating units told OIG they had such access controls in most systems. All nine operating units OIG examined have "external monitoring, security operations centers, intrusion detection systems/intrusion prevention systems, and event correlation tools." (18 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.
Cybersecurity Act of 2015 Report: CSB's Policies and Procedures to Protect Systems With Personally Identifiable Information	EPA Inspector General	August 1, 2016	The U.S. Chemical Safety Board (CSB) maintains one computer system that contains sensitive PII, according to the Environmental Protection Agency's inspector general. The audit, required under the Cybersecurity Act of 2015, includes a one-page summary of the findings "due to the sensitive nature of the information identified." The summary did not say if the audit had flagged security problems at CSB. The EPA inspector general has oversight of CSB, an independent agency. The inspector general's office examined eight areas of the system, including how CSB controls access to the system and looks for signs of external intrusions. (1 pages)
Report on the Department of Justice's Cybersecurity Logical Access Controls and Data Security Management Practices Pursuant to the Cybersecurity Act of 2015, Section 406, Federal Computer Security	DOJ Office of Inspector General	August 1, 2016	KPMG found that DOJ has developed policies and procedures to implement the controls addressed in Section 406 to establish an information security program compliant with NIST. For Logical Access Policies and Multi-

			factor Authentication, KPMG found that DOJ is making progress in implementing personal identity verification (PIV) logical access for privileged and unprivileged users across the organization, but significant work still needs to occur related to the PIV multi-factor implementation. (18 pages)
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 how—and if—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)
Agencies Need to Improve Controls over Selected High-Impact Systems	GAO	June 21, 2016	Federal systems categorized as high impact—those that hold sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harm—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 – 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 Uncertainties	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 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 Define Its Role in Responding to a Real-world Attack	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 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 Way Forward for Federal Background Investigations	FBI	January 22, 2016	The Obama Administration is creating a new organization within the Office of Personnel Management 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 list—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 Insurance Data Analytics System Needs Improvement	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 vulnerabilities—such as software bugs—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 Controls across Federal Agencies	GAO	June 24, 2015	This statement summarizes (1) challenges facing federal agencies in securing their systems and information and (2) government-wide initiatives, including those led by 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 challenges—including the hundreds of recommendations GAO and inspectors general made—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)
Review of Medicare Contractor Information Security Program Evaluations for Fiscal Year 2013	HHS, OIG	April 2015	The Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers (PwC) to 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. … 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 … 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 Practices	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 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 and Privacy Controls Should Be Enhanced to Address Weaknesses	GAO	September 18, 2014	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) 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 bureau—auditors do not say which—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 Enhanced	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 Unclassified Cyber Security Program - 2013	DOE OIG	October 2013	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 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. 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 schools—a requirement for becoming a joint staff officer and for promotion to the senior ranks—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)
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 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)—the federal agencies that oversee or provide support to the five types of field-based entities—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	GAO	January 25,	The Federal Communications Commission

Commission Needs to Strengthen Controls over Enhanced Secured Network Project		2013	(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)
The Department's Management of the Smart Grid Investment Grant Program	DOE OIG	January 20, 2012	According to the DOE' inspector general, the 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	GAO	July 29, 2011	The letter discusses DOD's cyber and information assurance budget for FY2012 and

Develop Full-Spectrum Cyberspace Budget Estimates			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 Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk	GAO	November 30, 2010	Existing government-wide guidelines and oversight efforts do not fully address agency implementation of leading wireless security practices. Until agencies take steps to better implement these leading practices and OMB takes steps to improve government-wide oversight, wireless networks will remain at an increased vulnerability to 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.
PERSEREC (Personnel and Security Research Center)	DOD	Continuously Updated	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 Information System for Security, or DISS, will consolidate two existing tools used for vetting employees and job applicants.

CyberSeek Tool	NIST	Continuously Updated	CyberSeek is an interactive online tool designed to make it easier for cybersecurity job seekers to find openings and for employers to identify the skilled workers they need.
CyberCareers.gov	OPM	Continuously Updated	The website is aimed at reaching federal managers, current employees, job seekers, and academic organizations and students. The site is designed as a one-stop shop to better educate those audiences about new federal cyber opportunities and provide resources to help them develop their careers in the field.
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.
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development	NIST	July 12, 2017	NIST is seeking information on the scope and sufficiency of efforts to educate and train the nation's cybersecurity workforce and recommendations for ways to support and improve that workforce in both the public and private sectors. (3 pages)
Federal Efforts Are Under Way That May Address Workforce Challenges	GAO	April 4, 2017	This statement discusses challenges agencies face in ensuring an effective cybersecurity workforce, recent initiatives aimed at improving the federal cyber workforce, and ongoing activities that could assist in recruiting and retaining cybersecurity professionals. In preparing this statement. (21 pages)
Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals	OPM	November 29, 2016	The guidance outlines the special rates under the General Schedule that can be paid to IT management and computer professionals, but also outlines other incentive tools. For example, agency leaders can offer up to 25% of annual pay bonus for retaining an employee and 10% for a group of employees. There are also relocation incentives and student loan repayment up to $60,000. (25 pages)
NICE Cybersecurity Workforce Framework (NCWF)	NISZT	November 2016	This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. It describes how the NCWF provides organizations with a common, consistent lexicon to categorize and describe cybersecurity work. The common lexicon provided by the NCWF enables consistent organization and communication about cybersecurity work. (130 pages)
Strengthening the Federal Cybersecurity Workforce	White House	July 12, 2016	The Strategy establishes four key initiatives: (1) Expand the Cybersecurity Workforce through Education and Training (2) Recruit the Nation's Best Cyber Talent for Federal Service (3) Retain and Develop Highly Skilled Talent (4) Identify Cybersecurity Workforce Needs.

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 Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction	(ISC)^2	April 17, 2015	In 2014, the average annual salary of a federal cybersecurity worker was $110,500, with federal contractors taking home $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. 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 schools—a requirement for becoming a joint staff officer and for promotion to the senior ranks—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 A—Cyber Operations-Related Military Occupations Appendix B—Commercial Certifications Supporting the DOD Information Assurance Workforce Improvement Program Appendix C—Military Services Training and Development Appendix D—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.
Statement by President Donald J. Trump on the Elevation of Cyber Command	White House	July 18, 2017	President Trump elevated U.S. Cyber Command to a full combatant command. The elevation will help streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander with authorities commensurate with the importance of such operations. Elevation will also ensure that critical cyberspace operations are adequately funded.
Federal Information Security Modernization Act of 2014: Annual Report to Congress (FY 2016)	OMB	March 10, 2017	Federal agencies reported 30,899 "cyber incidents" in fiscal 2016 that led to the "compromise of information or system functionality" to the Department of Homeland Security's U.S. Computer Emergency Readiness Team. (121 pages)

President-Elect Trump Announces Former Mayor Rudolph Giuliani to Lend Expertise to Cyber Security Efforts	White House	January 12, 2017	Former New York City Mayor Rudy Giuliani "will be sharing his expertise and insight as a trusted friend" on private-sector cyber security problems.
Report on Securing and Growing the Digital Economy	Commission on Enhancing National Cybersecurity	December 2016	President Obama "directed the Commission to assess the state of our nation's cybersecurity, and he charged this group with developing actionable recommendations for securing the digital economy. From these discussions, some firm conclusions emerged. Partnerships-between countries, between the national government and the states, between governments at all levels and the private sector-are a powerful tool for encouraging the technology, policies, and practices we need to secure and grow the digital economy. The Commission asserts that the joint collaboration between the public and private sectors before, during, and after a cyber event must be strengthened." (100 pages)
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 Budget—which is a part of EOP—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 National Action Plan	White House	February 9, 2016	The White House proposed a Cybersecurity National Action Plan, which provides a 35% increase in federal 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 Cybersecurity Efforts 2015	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 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 issue—industry, tech companies, law enforcement, consumer and privacy advocates, law professors who specialize in this field, and students—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.
Federal Information Security Management Act, Annual Report to Congress	OMB	May 1, 2014	The 24 largest federal departments and agencies spent $10.34 billion on cybersecurity in fiscal year 2014. The 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 year—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 of the Cybersecurity Framework	White House	August 6, 2013	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 – a set of core practices to 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 majority—90%—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 Federal Information Security Management Act and Agency Privacy Management	OMB	September 14, 2011	Rather than enforcing a static, three-year reauthorization 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	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

Leadership Is Needed			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)
Comprehensive National Cybersecurity Initiative (CNCI)	White House	March 2, 2010	The CNCI establishes a multipronged approach the 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 Rita Tehan.

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 organizations—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.
Cybersecurity Framework: Implementation Guidance for Federal Agencies, Interagency Report 8170	NIST	May 2017	The draft says federal agencies can use the cybersecurity framework to complement the existing suite of NIST security and privacy risk management standards, guidelines, and practices developed in response to the Federal Information Security Management Act. (41 pages)
Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (Request for Comment)	NIST	January 25, 2017	NIST has developed a draft update of the framework (termed "Version 1.1" or "V1.1"), available at http://www.nist.gov/cyberframework. The draft update seeks to clarify, refine, and enhance the framework, and make it easier to use, while retaining its flexible, voluntary, and cost-effective nature. The update will also be fully compatible with the February 2014 version of the framework in that either version may be used by organizations without degrading communication or functionality. NIST is soliciting

			public comments on this proposed update. Specifically, NIST is interested in comments that address updated features of the Framework. (2 pages)
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 Framework and the FTC	Federal Trade Commission	August 31, 2016	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 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 IoT—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)
Information Sharing and Analysis Organization	DHS	May 11, 2016	"This Notice announces a request for public comment on draft products produced by the Information Sharing and 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, Architecture, and High-Level Requirements	NIST	September 2014	The three-volume report presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information in the report as guidance for assessing risk and identifying and applying 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 § 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)—or "C-cubed"—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	NIST	August 28,	The framework provides a common language and

Cybersecurity Framework		2013	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 Partnership: A White Paper	Business Software Alliance, Center for Democracy and Technology, U.S. Chamber of Commerce, Internet Security Alliance, and Tech America	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 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	DHS	Continuously	CS&C

Communications (CS&C)		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 sector—the ".com" domain—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.
Mobile Device Security	DHS	April 2017	The study found that threats to the federal government's use of mobile devices—smartphones and tablet computers running mobile operating systems—exist across all elements of the mobile ecosystem. These threats require a security approach that differs substantially from the protections developed for desktop workstations largely because mobile devices are exposed to a distinct set of threats, frequently operate outside of enterprise protections and have evolved independently of desktop architectures. The study presents a series of recommendations to enhance the federal government's mobile device security. (125 pages)
Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems	GAO	March 28, 2017	DHS has initiatives for (1) detecting and preventing malicious cyber intrusions into agencies' networks and (2) deploying technology to assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities. In a January 2016 report, GAO made nine recommendations related to expanding NCPS's capability to detect cyber intrusions, notifying customers of potential incidents, providing analytic services, and sharing cyber-related information, among other things. DHS concurred with the recommendations and is taking actions to implement them. (16 pages)
Cybersecurity: Actions Needed to Strengthen U.S. Capabilities	GAO	February 1, 2017	"GAO recommends nine actions to DHS for enhancing the effectiveness and efficiency of NCCIC, including to determine the applicability of the implementing principles and establish metrics and methods for evaluating performance; and address identified impediments." (67 pages)
Critical Infrastructure Protection: Improvements Needed for DHS's Chemical Facility Whistleblower Report Process	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 objectives…. 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 department—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 Certain Information Security Controls	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 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 C³ Voluntary Program	Department of Homeland Security (DHS)	February 12, 2014	The C³ 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
DOD Cyber Strategy	DOD	Continuously Updated	The strategy guides the development of DOD's cyber forces and strengthens cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DOD's three primary cyber missions.
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.
PERSEREC (Personnel and Security Research Center)	DOD Office of People Analytics (OPA)	Continuously Updated	The Pentagon is slated to launch one mega database for investigating the trustworthiness of personnel who could have access to federal facilities and computer systems. The Defense Information System for Security, or DISS, will consolidate two existing tools used for vetting employees and job applicants.
Cyber Power Potential of the Army's Reserve Component	RAND	September 2017	This report identifies the number of Army RC cyber-skilled personnel to help identify ways in which these soldiers can be leveraged to conduct Army cyber operations. This report also describes the broader challenges and opportunities that the use of RC personnel presents. (206 pages)
DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened	GAO	August 1, 2017	The report examines (1) DOD officials' perspectives on the advantages and disadvantages of the dual-hat leadership arrangement of NSA/CSS and CYBERCOM, and actions that could mitigate risks if the leadership arrangement ends, and (2) the extent to which DOD has implemented key strategic cybersecurity guidance. GAO analyzed DOD cybersecurity strategies, guidance, and information and interviewed cognizant DOD officials. (46 pages)

Statement by President Donald J. Trump on the Elevation of Cyber Command	White House	July 18, 2017	President Trump elevated U.S. Cyber Command to a full combatant command. U.S. Cyber Command's elevation will also help streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander with authorities commensurate with the importance of such operations. Elevation will also ensure that critical cyberspace operations are adequately funded.
154th Cyber Protection Team engaged in network defense at Cybertropolis, Indiana	Army Cyber Command	March 2, 2017	The U.S. Army has created a realistic simulator that allows each member of the CPT to test, measure, and improve their cyberattack and defense skills and the team to build trust in each other. In a full-scale, small city in Butlerville, Indiana, called Cybertropolis, the team was challenged to conduct an interactive battle against attackers on the prison systems and, specifically, to detect and counter anti-virus evasion, network enumeration, ransomware, client-side attacks, pivoting, network service exploitation, privilege escalation, attacks against industrial control systems and Windows' domain attacks.
Cyber Supply Chain	Defense Science Board	February 2017	The task force addressed (1) practices to mitigate malicious supply chain risk and latent vulnerabilities, and whether opportunities exist to modify or strengthen these practices; (2) current department program protection processes, as well as other practices to detect and assess potential vulnerabilities in hardware and software; (3) the extent to which commercial off the shelf vulnerabilities have been reported and impact the security of DOD systems; and (4)• interagency activities that DOD could better leverage to reduce supply chain risks.
DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued from August 2015 Through July 31, 2016	DoD Office of Inspector General	December 13, 2016	Summarized DOD and Government Accountability Office audit reports issued from August 1, 2015, through July 31, 2016, that contained findings on DOD cybersecurity weaknesses. DOD and GAO issued 21 unclassified reports that addressed a wide range of cybersecurity weaknesses within DOD systems and networks. Reports issued during the reporting period most frequently cited cybersecurity weaknesses in the categories of risk management, identity and access management, security and privacy training, contractor systems, and configuration management. (40 pages)
Office of the Director Operational Test and Evaluation FY 2016 Annual Report	DOD	December 2016	DOD personnel too often treat network defense as an administrative function, not a war fighting capability. Until this paradigm changes, and the change is reflected in the department's approach to cybersecurity personnel, resource allocation, training, accountability, and program and network management, the department will continue to struggle to adequately defend its systems and networks from advanced cyberattacks. (532 pages)
DOD's Defense Industrial Base Cybersecurity Activities	DOD	October 4, 2016	This final rule responds to public comments and 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)
DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems	DoD Inspector General	August 15, 2016	As part of a review mandated by the 2015 Cybersecurity Act, DOD's inspector general offers summaries, not assessments of the department's policies and procedures on logical access control policies and practices, use of multifactor authentication, software inventory, threat prevention, and contractor oversight. (66 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 Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities	DOD Chief Information Officer	October 2, 2015	DOD is revising its DoD-DIB Cybersecurity (CS) Activities regulation to mandate reporting of cyber 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 recommendations —136—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)
Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense	National Guard	August 21, 2014	The results of this analysis reflect DOD's current view of its requirements for successful conduct of 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	DOD	May 6, 2013	China is using its computer network exploitation

Involving the People's Republic of China 2013 (Annual Report to Congress)			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 Detection at Multiple Scales (ADAMS)	Defense Advanced Research Projects Agency (DARPA)	November 9, 2011	The report describes a system for preventing leaks by 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 review—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 Attacks at Department of Defense Pose Increasing Risk	GAO	May 1996	Defense Information Systems Agency (DISA) estimates indicate that DOD may have been attacked 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.
Computer Security Portal	Continuously Updated	The portal covers electronic mail, Federal Information Processing Standards (FIPS), and Threats and Vulnerabilities.
Security and Privacy Controls for Information Systems and Organizations	August 2017	This publication provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. (494 pages)
Digital Identity Guidelines: Authentication and Lifecycle Management	June 2017	NIST is overhauling password guidelines. One revised recommendation is that IT departments should only force a password change when there's been a security breach. Another recommendation is to favor long phrases, rather than short passwords with special characters. There should no longer be a requirement to have a certain mix of special characters, upper case letters and numbers for a password. (78 pages)
Guide for Cybersecurity Event Recovery	December 2016	This publication provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. It also provides an example scenario that demonstrates guidance and informative metrics that may be helpful for improving resilience of information systems. (53 pages)

Domain Name Systems-Based Electronic Mail Security (NIST Cybersecurity Practice Guide)	November 2, 2016	The draft guide demonstrates how commercially available technologies can help email service providers improve the security of email communications. The practical, user-friendly guide shows members of the information security community how to implement example solutions intended to help them align more easily with relevant standards and best practices.
Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	November 2016	NIST formally unveiled their guidelines for increasing the security of internet-connected devices. The guide provides security guidelines for 30 different processes involved with managing internet connected devices, from the supply phase to testing. (257 pages)
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)
Two Cybersecurity Standards Come Together to Help Organizations Quantify and Prioritize Risk	August 11, 2016	NIST and FAIR are working together to help companies and governments entities use and implement the organizations' frameworks to mitigate cybersecurity risk in the most economical way. According to a FAIR Institute blog post, FAIR and NIST are fundamentally different but complimentary frameworks. NIST assesses the maturity level of cybersecurity risks by providing a list of good practices and FAIR assesses the amount of risk and activities that should be prioritized by an organization.
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 IoT— 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 Organizations: Building Effective Assessment Plans (SP 800-53A, rev. 4)	December 12, 2014	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 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

Rita Tehan, Senior Research Librarian (rtehan@crs.loc.gov, 7-6739)