Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity: Authoritative Reports and Resources, by Topic

Rita Tehan
Information Research Specialist

October 14, 2014

Congressional Research Service
7-5700
www.crs.gov
R42507

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

This report provides references to analytical reports on cybersecurity from CRS, other government agencies, trade associations, and interest groups. The reports and related websites are grouped under the following cybersecurity topics:

- policy overview
- National Strategy for Trusted Identities in Cyberspace (NSTIC)
- cloud computing and FedRAMP
- critical infrastructure
- cybercrime, data breaches, and data security
- national security, cyber espionage, and cyberwar (including Stuxnet)
- international efforts
- education/training/workforce
- research and development (R&D)

In addition, the report lists selected cybersecurity-related websites for congressional and government agencies, news, international organizations, and organizations or institutions.

Contents

Tables

Contacts

CRS Reports, by Topic[1]

This section provides references to analytical reports on cybersecurity from CRS, other government agencies, think tanks, trade associations, trade press, and technology research firms. For each topic, CRS reports are listed first, followed by tables with reports from other organizations.

CRS Reports and Other CRS Products: Cybersecurity Policy

- CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer
- CRS Report R41941, *The Obama Administration's Cybersecurity Proposal: Criminal Provisions*, by Gina Stevens
- CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.
- CRS Report R40150, *A Federal Chief Technology Officer in the Obama Administration: Options and Issues for Consideration*, by John F. Sargent Jr.
- CRS Report R42409, *Cybersecurity: Selected Legal Issues*, by Edward C. Liu et al.
- 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 Report R43015, *Cloud Computing: Constitutional and Statutory Privacy Protections*, by Richard M. Thompson II
- CRS Legal Sidebar WSLG478, House Intelligence Committee Marks Up Cybersecurity Bill CISPA, by Richard M. Thompson II
- CRS Legal Sidebar WSLG263, Can the President Deal with Cybersecurity Issues via Executive Order?, by Vivian S. Chu

[1] For information on legislation and hearings in the 112th-113th Congresses, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.

Table 1. Cybersecurity Overview

Title	Source	Date	Pages	Notes
How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts	RAND Corp.	June 27, 2014	33	Since the terrorist attacks of September 11, 2001, the sharing of intelligence and law enforcement information has been a central part of U.S. domestic security efforts. Though much of the public debate about such sharing focuses on addressing the threat of terrorism, organizations at all levels of government routinely share varied types of information through multiagency information systems, collaborative groups, and other links. 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, this 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 going forward.
Defending an Open, Global, Secure, and Resilient Internet	Council on Foreign Relations	June 2013	127	The Task Force recommends that the United States develop a digital policy framework based on four pillars, the last of which is that U.S.-based industry work rapidly to establish an industry-led approach to counter current and future cyberattacks.
Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity	Safegov.org, in coordination with the National Academy of Public Administration	March 2013	39	Report recommends that rather than periodically auditing whether an agency's systems meet the standards enumerated in Federal Information Security Management Act (FISMA) at a static moment in time, agencies and their inspectors general should keep running scorecards of "cyber risk indicators" based on continual IG assessments of a federal organization's cyber vulnerabilities.

Title	Source	Date	Pages	Notes
Developing a Framework To Improve Critical Infrastructure Cybersecurity (*Federal Register* Notice; Request for Information)	National Institute of Standards and Technology (NIST)	February 12, 2013	5	NIST announced the first step in the development of a Cybersecurity Framework, which will be a set of voluntary standards and best practices to guide industry in reducing cyber risks to the networks and computers that are vital to the nation's economy, security, and daily life.
SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project	Carnegie Mellon University	January 2013	23	This report addresses the endemic problem of functional cyber intelligence analysts not effectively communicating with non-technical audiences. It also notes organizations' reluctance to share information within their own entities, industries, and across economic sectors.
The National Cyber Security Framework Manual	NATO Cooperative Cyber Defense Center of Excellence	December 11, 2012	253	Provides detailed background information and in-depth theoretical frameworks to help the reader understand the various facets of National Cyber Security, according to different levels of public policy formulation. The four levels of government—political, strategic, operational and tactical/technical—each have their own perspectives on National Cyber Security, and each is addressed in individual sections within the Manual.
20 Critical Security Controls for Effective Cyber Defense	Center for Strategic & International Studies	November 2012	89	The top 20 security controls from a public-private consortium. Members of the Consortium include NSA, US CERT, DOD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DOD Cyber Crime Center plus commercial forensics experts in the banking and critical infrastructure communities.
Cyber Security Task Force: Public-Private Information Sharing	Bipartisan Policy Center	July 2012	24	Outlines a series of proposals that would enhance information sharing. The recommendations have two major components: (1) mitigation of perceived legal impediments to information sharing, and (2) incentivizing private sector information sharing by alleviating statutory and regulatory obstacles.
Cyber-security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness Around the World	McAfee and the Security Defense Agenda	February 2012	108	The report examines the current state of cyber-preparedness around the world, and is based on survey results from 80 policy-makers and cybersecurity experts in the government, business, and academic sectors from 27 countries. The countries were ranked on their state of cyber-preparedness.

Title	Source	Date	Pages	Notes
Mission Critical: A Public-Private Strategy for Effective Cybersecurity	Business Roundtable	October 11, 2011	28	Report suggests, "[p]ublic policy solutions must recognize the absolute importance of leveraging policy foundations that support effective global risk management, in contrast to "check-the-box" compliance approaches that can undermine security and cooperation." The document concludes with specific policy proposals and activity commitments.
World Cybersecurity Technology Research Summit (Belfast 2011)	Centre for Secure Information Technologies (CSIT)	September 12, 2011	14	The Belfast 2011 event attracted international cybersecurity experts from leading research institutes, government bodies, and industry who gathered to discuss current cybersecurity threats, predict future threats and the necessary mitigation techniques, and to develop a collective strategy for next research.
A Review of Frequently Used Cyber Analogies	National Security Cyberspace Institute	July 22, 2011	7	From the report, "The current cybersecurity crisis can be described several ways with numerous metaphors. Many compare the current crisis with the lawlessness to that of the Wild West and the out-dated tactics and race to security with the Cold War. When treated as a distressed ecosystem, the work of both national and international agencies to eradicate many infectious diseases serves as a model as how poor health can be corrected with proper resources and execution. Before these issues are discussed, what cyberspace actually is must be identified."
America's Cyber Future: Security and Prosperity in the Information Age	Center for a New American Security	May 31, 2011	296	To help U.S. policy makers address the growing danger of cyber insecurity, this two-volume report features chapters on cybersecurity strategy, policy, and technology by some of the world's leading experts on international relations, national security, and information technology.
Resilience of the Internet Interconnection Ecosystem	European Network and Information Security Agency (ENISA)	April 11, 2011	238	Part I: Summary and Recommendations; Part II: State of the Art Review (a detailed description of the Internet's routing mechanisms and analysis of their robustness at the technical, economic and policy levels.); Part III: Report on the Consultation (a broad range of stakeholders were consulted. This part reports on the consultation and summarizes the results). Part IV: Bibliography and Appendices.

Title	Source	Date	Pages	Notes
Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper	Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, Tech America	March 8, 2011	26	This 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*.
Cybersecurity Two Years Later	CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies	January 2011	22	From the report: "We thought then [in 2008] that securing cyberspace had become a critical challenge for national security, which our nation was not prepared to meet.... In our view, we are still not prepared."
Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop	National Research Council (NRC)	September 21, 2010	70	Discusses computer system security and privacy, their relationship to usability, and research at their intersection. This is drawn from remarks made at the National Research Council's July 2009 *Workshop on Usability, Security and Privacy of Computer Systems* as well as reports from the NRC's Computer Science and Telecommunications Board on security and privacy.
National Security Threats in Cyberspace	Joint Workshop of the National Security Threats in Cyberspace and the National Strategy Forum	September 15, 2009	37	The two-day workshop brought together more than two dozen experts with diverse backgrounds: physicists; telecommunications executives; Silicon Valley entrepreneurs; federal law enforcement, military, homeland security, and intelligence officials; congressional staffers; and civil liberties advocates. For two days they engaged in an open-ended discussion of cyber policy as it relates to national security, under Chatham House Rules: their comments were for the public record, but they were not for attribution.

Note: Highlights compiled by the Congressional Research Service (CRS) from the reports.

Table 2. National Strategy for Trusted Identities in Cyberspace (NSTIC)

Title	Source	Date	Pages	Notes
Identity Ecosystem Framework (IDESG)	IDESG	Ongoing	N/A	The NSTIC called for the establishment of a private sector-led steering group to administer the development and adoption of the Identity Ecosystem Framework: the IDESG. The IDESG receives its authority to operate from the active participation of its membership in accordance with the Rules of Association which follow. The IDESG has been initiated with the support of NIST. Following an initial period, the IDESG will transition to a self-sustaining organization.
NIST Awards Grants to Improve Online Security and Privacy	NIST	September 17, 2013	N/A	NIST announced more than $7 million in grants to support the NSTIC. The funding will enable five U.S. organizations to develop pilot identity protection and verification systems that offer consumers more privacy, security, and convenience online.
Five Pilot Projects Receive Grants to Promote Online Security and Privacy	NIST	September 20, 2012	N/A	NIST announced more than $9 million in grant awards to support the NSTIC. Five U.S. organizations will pilot identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information.
Recommendations for Establishing an Identity Ecosystem Governance Structure	NIST	February 17, 2012	51	NIST responds to comments received in response to the related Notice of Inquiry published in the *Federal Register* on June 14, 2011. This report summarizes the responses to the NOI and provides recommendations and intended government actions to serve as a catalyst for establishing such a governance structure. The recommendations result from comments and suggestions by the NOI respondents as well as best practices and lessons learned from similarly scoped governance efforts.
Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace	NIST	June 14, 2011	4	The department seeks public comment from all stakeholders, including the commercial, academic and civil society sectors, and consumer and privacy advocates on potential models, in the form of recommendations and key assumptions in the formation and structure of the steering group.
Administration Releases Strategy to Protect Online Consumers and Support Innovation and Fact Sheet on National Strategy for Trusted Identities in Cyberspace	White House	April 15, 2011	N/A	Press release on a proposal to administer the processes for policy and standards adoption for the Identity Ecosystem Framework in accordance with the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Title	Source	Date	Pages	Notes
National Strategy for Trusted Identities in Cyberspac	White House	April 15, 2011	52	The NSTIC aims to make online transactions more trustworthy, thereby giving businesses and consumers more confidence in conducting business online.
National Strategy for Trusted Identities in Cyberspac Options for Enhanced Online Security and Privacy (D	White House	June 25, 2010	39	The NSTIC, which is in response to one of the near term action items in the President's Cyberspace Policy Review, calls for the creation of an online environment, or an Identity Ecosystem, where individuals and organizations can complete online transactions with confidence, trusting the identities of each other and the identities of the infrastructure where transaction occur.

Note: Highlights compiled by CRS from the reports.

Table 3. Cloud Computing and FedRAMP

Title	Source	Date	Pages	Notes
About FedRAMP	General Services Administration	Ongoing	N/A	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.
The Department of Energy's Management of Cloud Computing Activities: Audit Report	Dept. of Energy Inspector General	September 1, 2014	20	DOE should do a better job buying, implementing and managing its cloud computing services. Programs and sites departmentwide have independently spent more than $30 million on cloud services, the inspector general report said, but the chief information officer's office could not accurately account for it.
Cloud Computing: The Concept, Impacts and the Role of Government Policy	Organization for Economic Co-operation and Development (OECD)	August 19, 2014	240	This report presents the concept of cloud computing, the services it provides and deployment models, and thus give a clear overview of what it is and what it is not. It provides an overview of how cloud computing changes the way computing is carried out, and evaluates the impacts of cloud computing (including its benefits and challenges as well as its economic and environmental impacts). Finally, the report discusses the policy issues raised by cloud computing and the role of governments and other stakeholders in addressing these issues.
Software Defined Perimeter	Cloud Security Alliance	December 1, 2013	13	The Software Defined Perimeter (SDP) initiative by the Cloud Security Alliance aims to make "invisible networks" accessible to a wider range of government agencies and corporations. The initiative will foster development of an architecture for securing the Internet of Things by using the cloud to create highly secure end-to-end networks between any IP-addressable entities.

Title	Source	Date	Pages	Notes
Delivering on the Promise of Big Data and the Cloud	Booz, Allen, Hamilton	January 9, 2013	7	From the report, "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."
Cloud Computing: An Overview of the Technology and the Issues facing American Innovators	House Judiciary Comm., Subcom. on Intellectual Property, Competition, and the Internet	July 25, 2012	156	Overview and discussion of cloud computing issues.
Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned	GAO	July 11, 2012	43	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 CIO to establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed in this report, as applicable.
Cloud Computing Strategy	DOD, Chief Information Officer	July 2012	44	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, and a service environment that can rapidly respond to changing mission needs.
A Global Reality: Governmental Access to Data in the Cloud—A Comparative Analysis of Ten International Jurisdictions	Hogan Lovells	May 23, 2012	13	This white paper compares the nature and extent of governmental access to data in the cloud in many jurisdictions around the world.
Policy Challenges of Cross-Border Cloud Computing	U.S. International Trade Commission	May 2012	38	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 that countries are addressing them through domestic policy making, international agreements, and other cooperative arrangements.

Title	Source	Date	Pages	Notes
Cloud Computing Synopsis and Recommendations (SP 800-146)	NIST	May 2012	81	NIST's guide explains cloud technologies in "plain terms" to federal agencies and provides recommendations for IT decision makers.
Global Cloud Computing Scorecard a Blueprint for Economic Opportunity	Business Software Alliance	February 2, 2012	24	This report notes that while 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.
Concept of Operations: FedRAMP	General Services Administration (GSA)	February 7, 2012	47	Implementation of FedRAMP will be in phases. This document describes all the services that will be available at initial operating capability—targeted for June 2012. The Concept of Operations will be updated as the program evolves toward sustained operations.
Federal Risk and Authorization Management Program (FedRAMP)	Federal CIO Council	January 4, 2012	N/A	FedRAMP has been established to provide a standard 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	7	FedRAMP will now be 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.
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)	NIST	December 1, 2011	32	Volume I is aimed at interested parties who 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.
U.S. Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters (SP 500-293)	NIST	December 1, 2011	85	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. Vol. II integrates and summarizes the work completed to date and explains how these findings support the roadmap introduced in Vol. I.

Title	Source	Date	Pages	Notes
Information Security: Additional Guidance Needed to Address Cloud Computing Concerns	GAO	October 6, 2011	17	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.
Cloud Computing Reference Architecture (SP 500-292)	NIST	September 1, 2011	35	This "Special Publication," which is not an official U.S. government standard, is designed to provide guidance to specific communities of practitioners and researchers.
Guide to Cloud Computing for Policy Makers	Software and Information Industry Association (SAII)	July 26, 2011	27	The SAII concludes "that there is no need for cloud-specific legislation or regulations to provide for the safe and rapid growth of cloud computing, and in fact, such actions could impede the great potential of cloud computing."
Federal Cloud Computing Strategy	White House	February 13, 2011	43	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.
25 Point Implementation Plan to Reform Federal Information Technology Management	White House	December 9, 2010	40	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.

Notes: These reports analyze cybersecurity issues related to the federal government's adoption of cloud computing storage options. Highlights compiled by CRS from the reports.

CRS Reports: Critical Infrastructure

- CRS Report R42683, *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, by John D. Moteff
- CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff
- CRS Report R42660, *Pipeline Cybersecurity: Federal Policy*, by Paul W. Parfomak
- CRS Report R41536, *Keeping America's Pipelines Safe and Secure: Key Issues for Congress*, by Paul W. Parfomak
- CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell
- CRS Report R42338, *Smart Meter Data: Privacy and Cybersecurity*, by Brandon J. Murrill, Edward C. Liu, and Richard M. Thompson II
- CRS Report RL33586, *The Federal Networking and Information Technology Research and Development Program: Background, Funding, and Activities*, by Patricia Moloney Figliola
- CRS Report 97-868, *Internet Domain Names: Background and Policy Issues*, by Lennard G. Kruger
- CRS Report IN10027, *Open-Source Software and Cybersecurity: The Heartbleed Bug*, by Eric A. Fischer, Catherine A. Theohary, and John W. Rollins

Table 4. Critical Infrastructure

Title	Source	Date	Pages	Notes
Cybersecurity for Energy Delivery Systems Program (CEDS)	Department of Energy, Office of Electricity Delivery & Energy Reliability	ongoing	N/A	The program assists the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.
Cybersecurity Capability Maturity Model (C2M2)	DOE Office of Electricity Delivery and Energy Reliability	ongoing	N/A	The model was developed by the DOE and industry as a cybersecurity control evaluation and improvement management tool for energy sector firms. Like the framework, it tells adherents to assess and grade adoption of cybersecurity practices.
GridEx	North American Electric Reliability Corporation (NERC)	ongoing	N/A	The objectives of the NERC Grid Security Exercise (GridEx) series are to use simulated scenarios (with NO real-world effects) to exercise the current readiness of participating Electricity Sub-sector entities to respond to cyber or physical security incidents and provide input for security program improvements to the bulk power system. GridEx is a biennial international grid security exercise that uses best practices and other contributions from the Department of Homeland Security, the Federal Emergency Management Agency, and the National Institute of Standards and Technology.
Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors	Senate Armed Services Committee	September 17, 2014	52	Hackers associated with the Chinese government successfully penetrated the computer systems of Transportation Command (TRANSCOM) contractors 20 times in the course of a single year. Chinese hackers tried to get into the systems 50 times. The congressional committee found that only two of the intrusions were detected. It also found that officials were unaware due in large part to unclear requirements and methods for contractors to report breaches and for government agencies to share information.
Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts	GAO	September 15, 2014	82	Homeland Security (DHS) used 10 different assessment tools and methods from FY2011 through FY2013 to assess critical infrastructure vulnerabilities. Four of the 10 assessments did not include cybersecurity. The differences in the assessment tools and methods mean DHS is not positioned to integrate its findings in identifying priorities.

Title	Source	Date	Pages	Notes
Energy Sector Cybersecurity Framework Implementation Guidance - Draft For Public Comment & Comment Submission Form	DOE Office of Electricity Delivery and Energy Reliability	September 12, 2014	N/A	Energy companies need not make a choice between the NIST cybersecurity framework and the DOE's Cybersecurity Capability Maturity Model. The NIST framework tells organizations to grade themselves on a four-tier scale based on their overall cybersecurity program sophistication. C2M2 tells users to assess cybersecurity control implementation across 10 "domains" of cybersecurity practices, such as "situational awareness," according to their specific "maturity indicator level."
Critical Infrastructure: Security Preparedness and Maturity	Unisys and Ponemon Institute	July 2014	34	Unisys and Ponemon Institute surveyed nearly 600 IT security executives of utility, energy, and manufacturing organizations. Overall, the report finds organizations are simply not prepared to deal with advanced cyber threats. Only half of companies have actually deployed IT security programs and, according to the survey, the top threat actually stems from negligent insiders.
Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid	Center for the Study of the Presidency and Congress	July 2014	180	"While [electrical grid] modernization entails significant challenges in its own right, it also provides an opportunity to 'bake security in'—both in the hardware and software controlling these systems and in the business models, regulatory systems, financial incentives, and insurance structures that govern the generation, transmission, and distribution of electric power. […] In this report and the aforementioned dozen recommendations, we have sought to identify the immediate action that can be taken by the White House, the Congress, and the private sector to mitigate current threats to the electrical grid."
Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity	GAO	June 5, 2014	54	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.
Executive Leadership of Cybersecurity: What Today's CEO Needs To Know About the Threats They Don't See	Federal Financial Institutions Examination Council (FFIEC)	May 7, 2014	30	FFIEC highlighted key focus areas for senior management and boards of directors of community institutions as they assess their institutions' abilities to identify and mitigate cybersecurity risks.

Title	Source	Date	Pages	Notes
Sector Risks Snapshots	Department of Homeland Security	May 2014	52	The Snapshots provide an introduction to the diverse array of critical infrastructure sectors, touching on some of the key threats and hazards concerning the sectors, and highlighting the common, first-order dependencies and interdependencies between sectors.
Critical Infrastructure Protection Issues Identified in Order No. 791	Federal Energy Regulatory Commission	April 24, 2014	N/A	FERC will hold a technical meeting on cybersecurity and communications security standards for power generators. Among other issues, the meeting will consider possible disjunctures between FERC's regulatory standards for grid reliability, and the new voluntary cybersecurity framework for critical infrastructure that was rolled out by the National Institute of Standards and Technology (NIST) earlier this year.
Notice of Completion of Notification of Cyber-Dependent Infrastructure and Process for Requesting Reconsideration of Determinations of Cyber Criticality	DHS Programs Directorate	April 17, 2014	3	The Secretary of DHS has been directed to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In addition to identifying such infrastructure, the Secretary has also been directed to confidentially notify owners and operators of critical infrastructure identified and establish a mechanism through which entities can request reconsideration of that identification, whether inclusion or exclusion from this list. This notice informs owners and operators of critical infrastructure that the confidential notification process is complete and describes the process for requesting reconsideration.
Cybersecurity Procurement Language for Energy Delivery Systems	DOE Energy Sector Control Systems Working Group	April 2014	46	The guidance suggests procurement strategies and contract language to help U.S. energy companies and technology suppliers "build in cybersecurity protections during product design and manufacturing. The guidance was "developed through a public-private working group including federal agencies and private industry leaders."
Benchmarking Trends: Interest in Cyber Insurance Continues to Climb (Requires free registration to access.)	Marsh USA	March 31, 2014	4	As cyber incidents increased in frequency and severity in 2013, the percentage of companies that purchased cyber insurance rose by double digits (see figure 1 in the report). Early signs in 2014 indicate that the trend is not just continuing but accelerating. Recent high-profile data breaches, growing board-level concern, and the increasing vulnerability of operations to failure of technology appear to be influencing purchasing decisions.

Title	Source	Date	Pages	Notes
Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat	Bipartisan Policy Center	February 28, 2014		BPC's initiative identifies urgent priorities, including strengthening existing protections, enhancing coordination at all levels, and accelerating the development of robust protocols for response and recovery in the event of a successful attack. The initiative developed recommendations in four policy areas: standards and best practices, information sharing, response to a cyberattack, and paying for cybersecurity. The recommendations are targeted to Congress, federal government agencies, state public utility commissions (PUCs), and industry.
Framework for Improving Critical Infrastructure Cybersecurity	NIST	February 12, 2014	41	The voluntary framework consists of cybersecurity standards that can be customized to various sectors and adapted by both large and small organizations. Additionally, so that the private sector may fully adopt this Framework, the Department of Homeland Security announced the Critical Infrastructure Cyber Community (C^3)—or "C-cubed"—Voluntary Program. The C^3 program gives companies that provide critical services like cell phones, email, banking, energy, and state and local governments, direct access to cybersecurity experts within DHS who have knowledge about specific threats, ways to counter those threats, and how, over the long term, to design and build systems that are less vulnerable to cyber threats.
ITI Recommendations to the Department of Homeland Security Regarding its Work Developing a Voluntary Program Under Executive Ordcer 163636, "Improving Critical Infrastructure Cybersecurity."	Information Technology Industry Council	February 11, 2014	3	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 a bigger biz argument, made in its report yesterday, is that ITI and others do not want incentives if they come at the cost of "compliance-based programs."

Title	Source	Date	Pages	Notes
The Federal Government's Track Record on Cybersecurity and Critical Infrastructure	Sen. Homeland Security and Governmental Affairs Committee (Minority Staff)	February 4, 2014	19	Since 2006, the federal government has spent at least $65 billion on securing its computers and networks, according to an estimate by the Congressional Research Service (CRS). The National Institute of Standards and Technology (NIST), the government's official body for setting cybersecurity standards, has produced thousands of pages of precise guidance on every significant aspect of IT security. And yet agencies—even agencies with responsibilities for critical infrastructure, or vast repositories of sensitive data—continue to leave themselves vulnerable, often by failing to take the most basic steps toward securing their systems and information.
NIPP 2013: Partnering for Critical Infrastructure Security and Resilience	Department of Homeland Security	2013	57	NIPP 2013 meets the requirements of Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, signed in February 2013. The Plan was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry. It provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes.
World Federation of Exchanges (WFE) Launches Global Cyber Security Committee	World Federation of Exchanges	December 12, 2013	N/A	The WFE announced the launch of the exchange industry's first cybersecurity committee with a mission to aid in the protection of the global capital markets. The working group will bring together representation from a number of exchanges and clearinghouses across the globe, to collaborate on best practices in global security.
The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities	Brookings Institution/ Center for 21st Century Security and Intelligence	July 2013	50	The study argues that the level of cybersecurity awareness and culture in U.S. port facilities is relatively low and that a cyberattack at a major U.S. port would quickly cause significant damage to the economy.
FFIEC Forms Cybersecurity and Critical Infrastructure Working Group	Federal Financial Institutions Examination Council (FFIEC)	June 6, 2013	2	FFIEC formed a working group to further promote coordination across the federal and state banking regulatory agencies on critical infrastructure and cybersecurity issues.
Electric Grid Vulnerability: Industry Responses Reveal Security Gaps	Rep. Edward Markey and Rep. Henry Waxman	May 21, 2013	35	The report found that less than a quarter of investor-owned utilities and less than half of municipal and cooperation-owned utilities followed through with voluntary standards issued by the Federal Energy Regulatory Commission after the Stuxnet worm struck in 2010.

Title	Source	Date	Pages	Notes
Initial Analysis of Cybersecurity Framework RFI Responses	NIST	May 20, 2013	33	Comments on the challenges of protecting the nation's critical infrastructure have identified a handful of issues for the more than 200 people and organizations who responded to a formal request for information. NIST has released an initial analysis of 243 responses to the Feb. 26 RFI. The analysis will form the basis for an upcoming workshop at Carnegie Mellon University in Pittsburgh as NIST moves forward on creating a cybersecurity framework for essential energy, utility, and communications systems.
Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, Notice of Request for Information	General Services Administration	May 13, 2013	3	Among other things, PPD–21 requires the General Services Administration, 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.
2013 Annual Report	Financial Stability Oversight Council (FSOC)	April 25, 2013	195	Under the Dodd-Frank Act, the Council must report annually to Congress on a range of issues, including significant financial market and regulatory developments, and potential emerging threats to the financial stability of the United States.The Council's recommendations address heightened risk management and supervisory attention to operational risks, including cybersecurity and infrastructure.
Version 5 Critical Infrastructure Protection Reliability Standards (Notice of Proposed Rulemaking)	Federal Energy Regulatory Commission	April 24, 2013	18	FERC proposes to approve the Version 5 Critical Infrastructure Protection Reliability Standards, CIP-002-5 through CIP-011-1, submitted by the North American Electric Reliability Corporation, the commission-certified Electric Reliability Organization. The proposed Reliability Standards, which pertain to the cybersecurity of the bulk electric system, represent an improvement over the current commission-approved CIP Reliability Standards as they adopt new cybersecurity controls and extend the scope of the systems that are protected by the CIP Reliability Standards.

Title	Source	Date	Pages	Notes
Wireless Cybersecurity	Syracuse University New York, Dept. of Electrical Engineering and Computer Science	April 2013	167	This project dealt with various threats in wireless networks, including: eavesdropping in a broadcast channel, non-cooperative eavesdropping in a single-source single-sink planar network, and primary user emulation attack in a cognitive radio network. The major contributions were: detailed analysis of performance trade-off in the presence of the eavesdropping threat; a combined encoding and routing approach that provides provable security against non-cooperating eavesdropping; and a physical layer approach to counter the primary emulation attack. The research results under this effort significantly advanced our understanding on some of the fundamental trade-offs among various performance metrics in a wireless system. Practically feasible wireless security measures were also obtained that could lead to more assured operations in which secured wireless networks play an indispensable role. This project led to one PhD dissertation, one pending patent application, two archival journal papers and a number of peer-reviewed conference papers.
Incentives To Adopt Improved Cybersecurity Practices	NIST and the National Telecommunica-tions and Information Administration	March 28, 2013	N/A	The Department of Commerce (DOC) is investigating ways to incentivize companies and organizations to improve their cybersecurity. To better understand what stakeholders—such as companies, trade associations, academics and others—believe would best serve as incentives, the department has released a series of questions to gather public comments in a Notice of Inquiry.
Cybersecurity: The Nation's Greatest Threat to Critical Infrastructure	U.S. Army War College	March 2013	38	This paper provides a background of what constitutes national critical infrastructure and Critical Infrastructure Protection (CIP); discusses the immense vulnerabilities, threats, and risks associated in the protection of critical infrastructure; and outlines governance and responsibilities of protecting vulnerable infrastructure. The paper makes recommendations for federal responsibilities and legislation to direct nation critical infrastructure efforts to ensure national security, public safety, and economic stability.
SCADA and Process Control Security Survey	SANS Institute	February 1, 2013	19	SANS Institute surveyed professionals who work with SCADA and process control systems. Of the nearly 700 respondents, 70% said they consider their SCADA systems to be at high or severe risk; one-third of them suspect that they have been already been infiltrated.

Title	Source	Date	Pages	Notes
Follow-up Audit of the Department's Cyber Security Incident Management Program	U.S. Department of Energy Inspector General's Office	December 2012	25	In 2008, the Department's Cyber Security Incident Management Program (DOE/IG-0787, January 2008) reported the department and National Nuclear Security Administration (NNSA) 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 incident management program and adversely affected the ability of law enforcement to investigate incidents. In response to the finding, management concurred with the recommendations and indicated that it had initiated actions to address the issues identified.
Terrorism and the Electric Power Delivery System	National Academies of Science	November 2012	146	Focuses on measures that could make the electric power delivery system less vulnerable to attacks, restore power faster after an attack, and make critical services less vulnerable when the delivery of conventional electric power has been disrupted.
New FERC Office to Focus on Cyber Security	U.S. Department of Energy	September 20, 2012	N/A	The Federal Energy Regulatory Commission (FERC) announced the creation of the agency's new Office of Energy Infrastructure Security, which will work to reduce threats to the electric grid and other energy facilities. The goal is for the office to help FERC, and other agencies and private companies, better identify potential dangers and solutions.
Canvassing the Targeting of Energy Infrastructure: The Energy Infrastructure Attack Database	Journal of Energy Security	August 7, 2012	8	The Energy Infrastructure Attack Database (EIAD) is a non-commercial dataset that structures information on reported (criminal and political) attacks to energy infrastructure (EI) (worldwide) since 1980, by non-state actors. In building this resource, the objective was to develop a product that could be broadly accessible and also connect to existing available resources.
Smart-Grid Security	Center for Infrastructure Protection and Homeland Security, George Mason School of Law	August 2012	26	Highlights the significance of and the challenges with securing the smart grid.

Title	Source	Date	Pages	Notes
Cybersecurity: Challenges in Securing the Electricity Grid	GAO	July 17, 2012	25	In a prior report, GAO made recommendations related to electricity grid modernization efforts, including developing an approach to monitor compliance with voluntary standards. These recommendations have not yet been implemented.
Energy Department Develops Tool with Industry to Help Utilities Strengthen Their Cybersecurity Capabilities	U.S. Department of Energy	June 28, 2012	N/A	The Cybersecurity Self-Evaluation Tool uses best practices that were developed for the Electricity Subsector Cybersecurity Capability Maturity Model Initiative, which involved a series of workshops with the private sector to draft a maturity model that can be used throughout the electric sector to better protect the grid.
ICS-CERT Incident Response Summary Report, 2009-2011	U.S. Industrial Control System Cyber Emergency Response Team (ICS-CERT)	May 9, 2012	17	The number of reported cyberattacks on U.S. critical infrastructure increased sharply—from 9 incidents in 2009 to 198 in 2011; water sector-specific incidents, when added to the incidents that affected several sectors, accounted for more than half of the incidents; in more than half of the most serious cases, implementing best practices such as login limitation or properly configured firewall, would have deterred the attack, reduced the time it would have taken to detect an attack, and minimize its impact.
Cybersecurity Risk Management Process (Electricity Subsector)	Department of Energy, Office of Electricity Delivery & Energy Reliability	May 2012	96	The guideline describes a risk management process that is targeted to the specific needs of electricity sector organizations. The objective of the guideline is to build upon existing guidance and requirements to develop a flexible risk management process tuned to the diverse missions, equipment, and business needs of the electric power industry.
ICT Applications for the Smart Grid: Opportunities and Policy Implications	Organization for Economic Co-operation and Development (OECD)	January 10, 2012	44	This report discusses "smart" applications of information and communication technologies (ICTs) for more sustainable energy production, management and consumption. The report outlines policy implications for government ministries dealing with telecommunications regulation, ICT sector and innovation promotion, and consumer and competition issues.
The Department's Management of the Smart Grid Investment Grant Program	Department of Energy (DOE) Inspector General	January 20, 2012	21	According to the Inspector General, DOE'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.

Title	Source	Date	Pages	Notes
Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use	Government Accountability Office (GAO)	December 9, 2011	77	According to GAO, given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the available guidance could help both federal and private-sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.
The Future of the Electric Grid	Massachusetts Institute of Technology (MIT)	December 5, 2011	39	Chapter 1 provides an overview of the status of the grid, the challenges and opportunities it will face, and major recommendations. To facilitate selective reading, detailed descriptions of the contents of each section in Chapters 2–9 are provided in each chapter's introduction, and recommendations are collected and briefly discussed in each chapter's final section. (See Chapter 9, Data Communications, Cybersecurity, and Information Privacy, pages 208-234).
FCC's Plan for Ensuring the Security of Telecommunications Networks	Federal Communications Commission (FCC)	June 3, 2011	1	FCC Chairman Genachowski's response to letter from Rep. Anna Eshoo dated November 2, 2010, re: concerns about the implications of foreign-controlled telecommunications infrastructure companies providing equipment to the U.S. market.
Cyber Infrastructure Protection	U.S. Army War College	May 9, 2011	324	Part 1 deals with strategic and policy cybersecurity-related issues and discusses the theory of cyberpower, Internet survivability, large scale data breaches, and the role of cyberpower in humanitarian assistance. Part 2 covers social and legal aspects of cyber infrastructure protection and discusses the attack dynamics of political and religiously motivated hackers. Part 3 discusses the technical aspects of cyber infrastructure protection, including the resilience of data centers, intrusion detection, and a strong emphasis on Internet protocol (IP) networks.
In the Dark: Crucial Industries Confront Cyberattacks	McAfee and Center for Strategic and International Studies (CSIS)	April 21, 2011	28	The study reveals an increase in cyberattacks on critical infrastructure such as power grids, oil, gas, and water; the study also shows that that many of the world's critical infrastructures lacked protection of their computer networks, and reveals the cost and impact of cyberattacks.

Title	Source	Date	Pages	Notes
Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems	Government Accountability Office (GAO)	March 16, 2011	17	According to GAO, executive branch agencies have made progress instituting several government-wide initiatives that are aimed at bolstering aspects of federal cybersecurity, such as reducing the number of federal access points to the Internet, establishing security configurations for desktop computers, and enhancing situational awareness of cyber events. Despite these efforts, the federal government continues to face significant challenges in protecting the nation's cyber-reliant critical infrastructure and federal information systems.
Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security	Department of Energy Office of Inspector General	January 26, 2011	30	NERC developed Critical Infrastructure Protection (CIP) cybersecurity reliability standards which were approved by the 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.
Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed	Government Accountability Office (GAO)	January 12, 2011	50	"To reduce the risk that NIST's smart grid cybersecurity guidelines will not be as effective as intended, the Secretary of Commerce should direct the Director of NIST to finalize the agency's plan for updating and maintaining the cybersecurity guidelines, including ensuring it incorporates (1) missing key elements identified in this report, and (2) specific milestones for when efforts are to be completed. Also, as a part of finalizing the plan, the Secretary of Commerce should direct the Director of NIST to assess whether any cybersecurity challenges identified in this report should be addressed in the guidelines."
Partnership for Cybersecurity Innovation	White House (Office of Science & Technology Policy)	December 6, 2010	4	The Obama Administration released a Memorandum of Understanding signed by DOC's NIST, DHS's Science and Technology Directorate (DHS/S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement is to speed up the commercialization of cybersecurity research innovations that support the nation's critical infrastructures.

Title	Source	Date	Pages	Notes
WIB Security Standard Released	International Instrument Users Association (WIB)	November 10, 2010		The Netherlands-based WIB, an international organization that represents global manufacturers in the industrial automation industry, announced the second version of the Process Control Domain Security Requirements For Vendors document—the first international standard that outlines a set of specific requirements focusing on cybersecurity best practices for suppliers of industrial automation and control systems.
Information Security Management System for Microsoft Cloud Infrastructure	Microsoft	November 2010	15	This study describes the standards Microsoft follows to address current and evolving cloud security threats. It also depicts the internal structures within Microsoft that handle cloud security and risk management issues.
NIST Finalizes Initial Set of Smart Grid Cyber Security Guidelines	National Institute of Standards and Technology (NIST)	September 2, 2010	N/A	NIST released a three-volume set of recommendations relevant to securing the Smart Grid. The guidelines address a variety of topics, including high-level security requirements, a risk assessment framework, an evaluation of privacy issues in residences and recommendations for protecting the evolving grid from attacks, malicious code, cascading errors, and other threats.
Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed	Government Accountability Office (GAO)	July 15, 2010	38	Private-sector stakeholders reported that they expect their federal partners to provide usable, timely, and actionable cyber threat information and alerts; access to sensitive or classified information; a secure mechanism for sharing information; security clearances; and a single centralized government cybersecurity organization to coordinate government efforts. However, according to private sector stakeholders, federal partners are not consistently meeting these expectations.
The Future of Cloud Computing	Pew Research Center's Internet & American Life Project	June 11, 2010	26	Technology experts and stakeholders expect they will "live mostly in the cloud" in 2020 and not on the desktop, working mostly through cyberspace-based applications accessed through networked devices.
The Reliability of Global Undersea Communications Cable Infrastructure (The ROGUCCI Report)	IEEE/EastWest Institute	May 26, 2010	186	This study submits 12 major recommendations to private sector, governments and other stakeholders—especially the financial sector—for the purpose of improving the reliability, robustness, resilience, and security of the world's undersea communications cable infrastructure.

Title	Source	Date	Pages	Notes
NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses	Department of Energy, Idaho National Laboratory	May 2010	123	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.
Explore the reliability and resiliency of commercial broadband communications networks	Federal Communications Commission (FCC)	April 21, 2010	N/A	The FCC launched an inquiry into the ability of existing broadband networks to withstand significant damage or severe overloads as a result of natural disasters, terrorist attacks, pandemics or other major public emergencies, as recommended in the National Broadband Plan.
Security Guidance for Critical Areas of Focus in Cloud Computing V2.1	Cloud Security Alliance	December 2009	76	From the report, "Through our focus on the central issues of cloud computing security, we have attempted to bring greater clarity to an otherwise complicated landscape, which is often filled with incomplete and oversimplified information. Our focus ... serves to bring context and specificity to the cloud computing security discussion: enabling us to go beyond gross generalizations to deliver more insightful and targeted recommendations."
21 Steps to Improve Cyber Security of SCADA Networks	U.S. Department of Energy, Infrastructure Security and Energy Restoration	January 1, 2007	10	The President's Critical Infrastructure Protection Board and the Department of Energy have developed steps to help any organization improve the security of its SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.

Note: Highlights compiled by CRS from the reports.

CRS Reports and Other CRS Products: Cybercrime and National Security

- CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle
- CRS Report 94-166, *Extraterritorial Application of American Criminal Law*, by Charles Doyle
- CRS Report R42403, *Cybersecurity: Cyber Crime Protection Security Act (S. 2111, 112th Congress)—A Legal Analysis*, by Charles Doyle
- CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle
- CRS Report RL32706, *Spyware: Background and Policy Issues for Congress*, by Patricia Moloney Figliola
- CRS Report CRS Report R41975, *Illegal Internet Streaming of Copyrighted Content: Legislation in the 112th Congress*, by Brian T. Yeh
- CRS Report R42112, *Online Copyright Infringement and Counterfeiting: Legislation in the 112th Congress*, by Brian T. Yeh
- CRS Report R40599, *Identity Theft: Trends and Issues*, by Kristin Finklea
- CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea
- CRS Report RL34651, *Protection of Children Online: Federal and State Laws Addressing Cyberstalking, Cyberharassment, and Cyberbullying*, by Alison M. Smith
- CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary
- CRS Report R43382, *Data Security and Credit Card Thefts: CRS Experts*, by Eric A. Fischer
- CRS Legal Sidebar WSLG399, Legal Barriers to an Expanded Role of the Military in Defending Against Domestic Cyberattacks, by Andrew Nolan
- CRS Legal Sidebar WSLG483, Obstacles to Private Sector Cyber Threat Information Sharing, by Edward C. Liu and Edward C. Liu
- CRS Legal Sidebar WSLG672, Online Banking Fraud: Liability for Unauthorized Payment from Business Checking Account, by M. Maureen Murphy
- CRS Legal Sidebar WSLG831, Federal Securities Laws and Recent Data Breaches, by Michael V. Seitzinger
- CRS Legal Sidebar WSLG 906, Hackers Cannot Always Be Tried Where Third-Party Victims Reside, by Charles Doyle
- CRS Legal Sidebar WSLG 959, *In the Matter of LabMD*: The FTC Must Publicly Disclose Its Data Security Standards, by Gina StevensObst

Table 5. Cybercrime, Data Breaches, and Data Security

Title	Source	Date	Pages	Notes
ThreatWatch	NextGov	Ongoing	N/A	ThreatWatch is a snapshot of the data breaches hitting organizations and individuals, globally, on a daily basis. It is not an authoritative list, since many compromises are never reported or even discovered. The information is based on accounts published by outside news organizations and researchers.
Criminal Underground Economy Series	Trend Micro	Ongoing	N/A	A review of various cybercrime markets around the world.
2014 Cost of Cybercrime Global Report (email registration required)	HP Enterprise Security and Ponemon Institute	October 8, 2014	30	The 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, up from 32 days in 2013.
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 organization cost of more than $5 million. But in the end, it is the customers who are picking up the tab, from higher retail costs to credit card reissue fees.
Is Ransomware Poised for Growth?	Symantec	July 14, 2014	N/A	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 to unlock it the victim would have to pay a fine—often between $100-$500. Ransomware escalated in 2013, with a 500% (6-fold) increase in attack numbers between the start and end of the year.
iDATA: Improving Defences Against Targeted Attack	Centre for the Protection of National Infrastructure (UK)	July 2014	8	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 a number of outputs for the cyber security community. This document provides a description of the iDATA program and a summary of the reports.
Cyber Risks: The Growing Threat	Insurance Information Institute	June 27, 2014	27	Despite that cyber risks and cyber security are widely acknowledged to be a serious threat, many companies today still do not purchase cyber risk insurance.... Specialist cyber insurance policies have been developed by insurers 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.

Title	Source	Date	Pages	Notes
Hackers Wanted: An Examination of the Cybersecurity Labor Market	RAND Corp.	June 24, 2014	110	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.
Global Cybercrime: The Interplay of Politics and Law	Centre for International Governance Innovation (CIGI)	June 20, 2014	23	This paper explores the recent unsealing of a 31-count indictment against five Chinese government officials and a significant cyber breach, perpetrated by Chinese actors against Western oil, energy, and petrochemical companies. The paper concludes by noting that increased cooperation among governments is necessary, but unlikely to occur as long as the discourse surrounding cybercrime remains so heavily politicized and securitized. If governments coalesced around the notion of trying to prevent the long-term degradation of trust in the online economy, they may profitably advance the dialogue away from mutual suspicion and toward mutual cooperation.
Net Losses: Estimating the Global Cost of Cybercrime	Center for Strategic and International Studies and McAfee	June 2014	24	This report explores the economic impact of cybercrime, including estimation, regional variances, IP theft, opportunity and recovery costs, and the future of cybercrime.
2014 U.S. State of Cybercrime Survey	PwC, CSO Magazine, the CERT Division of the Software Engineering Institute at Carnegie Mellon University, and the U.S. Secret Service	May 29, 2014	21	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 in four (77%) respondents to the survey detected a security event in the past 12 months, and more than a third (34%) said the number of security incidents detected increased over the previous year.
Privileged User Abuse & The Insider Threat (Requires free registration to access.)	Ponemon Institute and Raytheon	May 21, 2014	32	The report looks at what companies are doing right and the vulnerabilities that need to be addressed with policies and technologies. One area that is a big problem is the difficulty in actually knowing if an action taken by an insider is truly a threat. Sixty-nine percent of respondents say they don't have enough contextual information from security tools to make this assessment and 56% say security tools yield too many false positives.

Title	Source	Date	Pages	Notes
Online Advertising and Hidden Hazards to Consumer Security and Data Privacy	Senate Permanent Subcommittee on Investigations	May 15, 2014	47	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.
Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)	Department of Justice	May 9, 2014	7	The Department of Justice 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 whitepaper says that the law does not prohibit companies from divulging data in the aggregate, without any specific details about identifiable customers.
The Rising Strategic Risks of Cyberattacks	McKinsey & Company	May 2014	N/A	Companies are struggling with their capabilities in cyberrisk management. As highly visible breaches occur with growing regularity, most technology executives believe that 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	85	The 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.
The Target Breach, by the Numbers	Krebs on Security	May 6, 2014	N/A	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, amount of money Target estimates it will spend upgrading payment terminals to support Chip-and-PIN enabled cards).
Heartbleed's Impact	Pew Research Center	April 30, 2014	13	The Heartbleed security flaw on one of the most widely used "secure socket" encryption programs on the Internet had an impact on a notable share of Internet users. Some 60% of adults (and 64% of Internet users) said they had heard about the bug. Some 19% of adults said they had heard "a lot" about it and 41% said they had heard "a little" about it. By comparison, though, the Heartbleed story drew much less intensity and scope of attention than other big news stories.

Title	Source	Date	Pages	Notes
Russian Underground Revisited	Trend Micro	April 28, 2014	25	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 not a result of declining demand, but rather shows the result of an increasingly sophisticated marketplace. This report outlines the products and services being sold and what their prices are.
A "Kill Chain" Analysis of the 2013 Target Data Breach	Senate Commerce Committee	March 26, 2014	18	This 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 today widely used by information security professionals in both the public and the private sectors. This analysis suggests that Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach.
Markets for Cybercrime Tools and Stolen Data	RAND Corp. National Security Research Division and Juniper Networks	March 25, 2014	83	This 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.
Merchant and Financial Trade Associations Announce Cybersecurity Partnership	Retail Industry Leaders Association	February 13, 2014	N/A	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 (RILA) and the Financial Services Roundtable (FSR), joined by the American Bankers Association (ABA), the American Hotel & Lodging Association (AH&LA), The Clearing House (TCH), the Consumer Bankers Association (CBA), the Food Marketing Institute (FMI), the Electronic Transactions Association (ETA), the Independent Community Bankers of America (ICBA), the International Council of Shopping Centers (ICSC), the National Associations of Convenience Stores (NACS), the National Grocers Association (NGA), the National Restaurant Association (NRA), and the National Retail Federation (NRF).

Title	Source	Date	Pages	Notes
FTC Statement Marking the FTC's 50th Data Security Settlement	Federal Trade Commission	January 31, 2014	2	The FTC announces 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 protections for consumers and has encouraged companies to make safeguarding consumer data a priority.
Worst Practices Guide to Insider Threats: Lessons from Past Mistakes	American Academy of Arts & Sciences	January 2014	32	From the report: "Here, we are presenting a kind of 'worst practices' guide of serious mistakes made in the past regarding insider threats. While each situation is unique, and serious insider problems are relatively rare, the incidents we describe reflect issues that exist in many contexts and that every nuclear 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."
ENISA Threat Landscape 2013 – Overview of Current and Emerging Cyber-Threats	European Union Agency for Network and Information Security (ENISA)	December 11, 2013	70	The report is a collection of top cyber-threats that have been assessed in the reporting period (i.e., within 2013). ENISA has collected over 250 reports regarding cyber-threats, risks, and threat agents. ETL 2013 is a comprehensive compilation of the top 15 cyber-threats assessed.
Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences	Brookings Institution	December 2013	18	Economic espionage has existed at least since the industrial revolution, but the scope of modern cyber-enabled competitive data theft may be unprecedented. With this paper, Friedman, Mack-Crane, and Hammond 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.
Trends in Incident Response in 2013	ICS-CERT Monitor	October-December 2013	14	In 2013, ICS-CERT responded to 256 incidents reported either directly from asset owners or through other trusted partners. The majority of these incidents were initially detected in business networks of critical infrastructure organizations that operate industrial control systems (ICS). Of the 256 reported incidents, 59%, or 151 incidents, occurred in the energy sector, which exceeded all incidents reported in other sectors combined.

Title	Source	Date	Pages	Notes
Illicit Cyber Activity Involving Fraud	Carnegie Mellon University Software Engineering Institute	August 8, 2013	28	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 sector.
The Economic Impact of Cybercrime and Cyber Espionage	Center for Strategic and International Studies	July 22, 2013	20	Losses to the United States (the country where 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.
Cyber-Crime, Securities Markets, and Systemic Risk	World Federation of Exchanges (WFE) and the International Organization of Securities Commissions (IOSCO)	July 16, 2013	59	This report explores the nature and extent of cyber-crime in securities markets so far; the potential systemic risk aspects of this threat; and presents the results of a survey to the world's exchanges on their experiences with cyber-crime, cyber-security practices and perceptions of the risk.
Towards Trustworthy Social Media and Crowdsourcing	Wilson Center	May 2013	12	Individuals and organizations interested in using social media and crowdsourcing currently lack two key sets of information: a systematic assessment of the vulnerabilities in these technologies and a comprehensive set of best practices describing how to address those vulnerabilities. Identifying those vulnerabilities and developing those best practices are necessary to address a growing number of cybersecurity incidents ranging from innocent mistakes to targeted attacks that have claimed lives and cost millions of dollars.
Remaking American Security: Supply Chain Vulnerabilities & National Security Risks Across the U.S. Defense Industrial Base	Alliance for American Manufacturing	May 2013	355	Because the supply chain is global, it makes sense for U.S. officials to cooperate with other nations to ward off cyberattacks. Increased international cooperation to secure the integrity of the global IT system is a valuable long-term objective.
Comprehensive Study on Cybercrime	United Nations Office on Drugs and Crime (UNODC)	February 2013	320	The Study examined the problem of cybercrime from the perspective of governments, the private sector, academia and international organizations. The results are presented in eight Chapters, covering Internet connectivity and cybercrime; the global cybercrime picture; cybercrime legislation and frameworks; criminalization of cybercrime; law enforcement and cybercrime investigations; electronic evidence and criminal justice; international cooperation in criminal matters involving cybercrime; and cybercrime prevention.

Title	Source	Date	Pages	Notes
HoneyMap - Visualizing Worldwide Attacks in Real-Time, and Honeynet Map	The Honeynet Project	October 1, 2012	N/A	The HoneyMap shows a real-time visualization of attacks against the Honeynet Project's sensors deployed around the world.
Does Cybercrime Really Cost $1 Trillion?	ProPublica	August 1, 2012	N/A	In a news release to announce its 2009 report, "Unsecured Economies: Protecting Vital Information," computer security firm McAfee estimated a trillion dollar global cost for cybercrime. The number does not appear in the report itself. McAfee's trillion-dollar 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 of their origins 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.
Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage	GAO	June 28, 2012	20	This 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 IP.
Measuring the Cost of Cybercrime	11th Annual Workshop on the Economics of Information Security	June 25, 2012	N/A	From the report, "For each of the main categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs - both to the UK and to the world as a whole."
The Impact of Cybercrime on Businesses	Ponemon Institute	May 2012	21	The study found that targeted attacks on businesses cost enterprises an average of $214,000. The expenses are associated with forensic investigations, investments in technology, and brand recovery costs.
Proactive Policy Measures by Internet Service Providers against Botnets	Organisation for Economic Co-operation and Development	May 7, 2012	25	This report analyzes initiatives in a number of countries through which end-users are notified by ISPs when their computer is identified as being compromised by malicious software and encouraged to take action to mitigate the problem.
Developing State Solutions to Business Identity Theft: Assistance, Prevention and Detection Efforts by Secretary of State Offices	National Association of Secretaries of State	January 2012	23	This 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.
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)	SANS	October 3, 2011	77	The 20 security measures are intended to focus agencies' limited resources on plugging the most common attack vectors.

Title	Source	Date	Pages	Notes
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	14	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).
The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis Bases on Spam Data	Organisation for Economic Co-operation and Development	November 12, 2010	31	This working paper considers whether ISPs can be critical control points for botnet mitigation, how the number of infected machines varies across ISPs, and why.
Untangling Attribution: Moving to Accountability in Cyberspace [Testimony]	Council on Foreign Relations	July 15, 2010	14	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 the privacy of Internet users.
Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities	National Research Council	2009	368	This report explores important characteristics of cyberattack. It describes the current international and domestic legal structure as it might apply to cyberattack, and considers analogies to other domains of conflict to develop relevant insights.

Note: Highlights compiled by CRS from the reports.

Table 6. National Security, Cyber Espionage, and Cyberwar

Title	Source	Date	Pages	Notes
Cyberthreat: Real-Time Map	Kaspersky Labs	Ongoing	N/A	Kaspersky Labs has launched an interactive cyberthreat 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 sub-systems.
The National Intelligence Strategy of the United States of America 2014	Office of the Director of National Intelligence	September 18, 2014	24	Cyber intelligence is one of four "primary topical missions" the intelligence community must accomplish. Both state and non-state 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," the strategy states. To become more effective in the cyber arena, the IC will improve its ability to correctly attribute attacks.
Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report	The Annenberg Public Policy Center and the Bipartisan Policy Center	July 22, 2014	48	Members of the panel that studied the 2001 attacks urge Congress to enact cybersecurity 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.
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	64	In the report, the author examines existing information technology security weaknesses and provides nine specific recommendations for the U.S. government and others to cope with these insecurities.
Baseline Review: ICT-Related Processes & Events, Implications for International and Regional Security (2011-2013)	ICT4Peace	May 1, 2014	50	The report is structured around the following three areas: (1) international and regional security (the predominant focus); (2) transnational crime and terrorism; and (3) governance, human rights and development. These areas are obviously interdependent, with developments in one area often impacting another, yet they have traditionally been approached separately through distinct communities of practice and fora. The report will serve as a baseline for future annual reports with this specific one covering the period spanning January 2011 to December 2013 (while also providing background on earlier events).

Title	Source	Date	Pages	Notes
M Trends: Beyond the Breach: 2014 Threat Report	Mandiant	April 2014	28	From the report, "One conclusion is inescapable: the list of potential targets has increased, and the playing field has grown, 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 decision makers. Private organizations have increasingly become collateral damage in political conflicts. With no diplomatic solution in sight, the ability to detect and respond to attacks has never been more important."
Emerging Cyber Threats Report 2014	Georgia Institute of Technology	January 2014	16	Brief compilation of academic research on Losing Control of Cloud Data, Insecure but Connected Devices, Attackers Adapt to Mobile Ecosystems, Costs of Defending Against Cyber Attacks Remain High, Information Manipulation Advances.
Cybersecurity and Cyberwar: What Everyone Needs to Know	Singer, Peter W. and Allan Friedman (Brookings Institution)	January 2014	306	The book looks at cybersecurity issues faced by the military, government, businesses and individuals, and what happens when they try to balance security with freedom of speech and the ideals of an open Internet.
Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences	Brookings Institution	December 2013	18	Economic espionage has existed at least since the industrial revolution, but the scope of modern cyber-enabled competitive data theft may be unprecedented. With this paper, Friedman, Mack-Crane, and Hammond 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.

Title	Source	Date	Pages	Notes
To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve	The Langner Group	November 2013	36	This document 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 especially provides an analysis of the bigger and much more complex payload that was designed to damage centrifuge rotors by overpressure. With both attack vectors viewed in context, conclusions are drawn about the reasoning behind a radical change of tactics between the complex earlier attack and the comparatively simple later attack that tried to manipulate centrifuge rotor speeds.
2013 Annual Report to Congress	U.S.-China Economic Commission	October 20, 2013	465	In 2013, the commission continued its close examination of China's cyber capabilities. Strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States, including the U.S. government and private companies. However, the public exposure of Chinese cyber espionage in 2013 has apparently not changed China's attitude about the use of cyber espionage to steal intellectual property and proprietary information. (See: Chapter 2, Section 2: "China's Cyber Activities.")
W32.Duqu: The Precursor to the Next Stuxnet	Symantec	November 14, 2013	N/A	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 which wreaked havoc in Iran's nuclear centrifuge farms last summer. 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 their initial findings, including analysis comparing the threat to Stuxnet.
Offensive Cyber Capabilities at the Operational Level - The Way Ahead	Center for Strategic & International Studies (CSIS)	September 16, 2013	20	The specific question this report examines is whether the Defense Department should make a more deliberate effort to explore the potential of offensive cyber tools at levels below that of a combatant command.

Title	Source	Date	Pages	Notes
Cyber-Warfare: Is the risk of cyber-warfare overrated?	The Economist	August 2, 2013	N/A	(*Economist Debates* adapt the Oxford style of debating to an online forum. Each side has three chances to persuade readers: opening, rebuttal and closing.) "Separating hype from the urgent questions is hard. Amid talk of a "digital Pearl Harbour" and "advanced persistent threats" it is hard to know whether we are really "losing the war" against the purveyors and users of malware and digital weapons."
The Economic Impact of Cybercrime and Cyber Espionage	Center for Strategic and International Studies	July 22, 2013	20	Losses to the United States (the country where 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.
Strategies for Resolving the Cyber Attribution Challenge	Air University, Maxwell Air Force Base	May 2013	109	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. This work builds on other appealing arguments for state responsibility in cyberspace.
Role of Counterterrorism Law in Shaping 'ad Bellum' Norms for Cyber Warfare	International Law Studies (U.S. Naval War College)	April 1, 2013	42	The prospect of cyber war has evolved from science fiction and over-the-top doomsday depictions on television, films, and in novels to reality and front-page news… 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.
The Tallinn Manual on the International Law Applicable to Cyber Warfare	Cambridge University Press/ NATO Cooperative Cyber Defence Center of Excellence	March 5, 2013	302	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 each rules' 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 each rules' application. (Note: The manual is not an official NATO publication, but an expression of opinions of a group of independent experts acting solely in their personal capacity.)

Title	Source	Date	Pages	Notes
Cyberterrorism: A Survey of Researchers	Swansea University	March 2013	21	This 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 and November 2012, and employed a questionnaire which was distributed to over 600 researchers, authors and other experts. Potential respondents were identified using a combination of methods, including targeted literature reviews, standing within relevant academic communities, snowballing from earlier participants or contacts, and the use of two mailing lists. 118 responses were received in total, from individuals working in 24 countries across six continents. Please contact the research team with any enquiries on the project's methods and findings (see p. 21 for contact details).
APT1: Exposing One of China's Cyber Espionage Units	Mandiant	February 19, 2013	76	The details analyzed during hundreds of investigations signal that the groups conducting these activities (computer security breaches around the world) are based primarily in China and that the Chinese government is aware of them.
Video demo of Chinese hacker activity (click on "APT1 Video" at top right of screen)	Mandiant	February 19, 2013	N/A	Video of APT1 attacker sessions and intrusion activities (5-minute video).
Responding to Cyber Attacks and the Applicability of Existing International Law	Army War College	January 2013	34	This 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. Finally, 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.
Crisis and Escalation in Cyberspace	RAND Corp.	December 2012	200	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, by controlling the narrative, understanding the stability parameters of the crises, and trying to manage escalation if conflicts arise from crises.

Title	Source	Date	Pages	Notes
Cyberattacks Among Rivals: 2001-2011 (from the article, "The Fog of Cyberwar" by Brandon Variano and Ryan Maness (subscription required)	Foreign Affairs	November 21, 2012	N/A	A chart showing cyberattacks by initiator and victim, 2001-2011.
Emerging Cyber Threats Report 2013	Georgia Institute of Technology	November 14, 2012	9	The year ahead will feature new and increasingly sophisticated means to capture and exploit user data, escalating battles over the control of online information and continuous threats to the U.S. supply chain from global sources. (From the annual Georgia Tech Cyber Security Summit 2012.)
Proactive Defense for Evolving Cyber Threats	Sandia National Labs	November 2012	98	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.
Safeguarding Cyber-Security, Fighting in Cyberspace	International Relations and Security Network (ISN)	October 22, 2012	N/A	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., one that believes 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	12	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.
Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE	House Permanent Select Committee on Intelligence	October 8, 2012	60	The committee initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States.
Federal Support for and Involvement in State and Local Fusion Centers	U.S. Senate Permanent Subcommittee on Investigations	October 3, 2012	141	A two-year bipartisan investigation found that U.S. Department of Homeland Security 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.

Title	Source	Date	Pages	Notes
Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States	First Monday	July 2, 2012	N/A	This essay argues that current contradictory tendencies 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 cyber war.
Nodes and Codes: The Reality of Cyber Warfare	U.S. Army School of Advanced Military Studies, Command and General Staff	May 17, 2012	62	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.
United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?	Triangle Institute for Security Studies	March 2012	34	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. Specifically, national CT cyber policies that are not completely sourced in domestic or international law unnecessarily limit the latitude cyber CT professionals need to effectively counter terrorists through the use of organic cyber capabilities. 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.
A Cyberworm that Knows No Boundaries	RAND	December 21, 2011	55	Stuxnet-like worms pose a serious threat even to infrastructure and computer systems that are not connected to the Internet. However, defending against such attacks is an increasingly complex prospect.
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	14	From the report: "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."
Cyber War Will Not Take Place	Journal of Strategic Studies	October 5, 2011	29	The paper argues that cyber warfare has never taken place, is not currently taking place, and is unlikely to take place in the future.

Title	Source	Date	Pages	Notes
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	31	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.
USCYBERCOM and Cyber Security: Is a Comprehensive Strategy Possible?	Army War College	May 12, 2011	32	Examine five aspects of USCYBERCOM: organization, command and control, computer network operations (CNO), synchronization, and resourcing. Identify areas that currently present significant risk to USCYBERCOM's ability to create a strategy that can achieve success in its cyberspace operations. Recommend potential solutions that can increase the effectiveness of the USCYBERCOM strategy.
A Four-Day Dive Into Stuxnet's Heart	Threat Level Blog (Wired)	December 27, 2010	N/A	From the article, "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? Preliminary Assessment	Institute for Science and International Security	December 22, 2010	10	This 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.
Stuxnet Analysis	European Network and Information Security Agency	October 7, 2010	N/A	EU cybersecurity agency warns that the Stuxnet malware is a game changer for critical information infrastructure protection; PLC controllers of SCADA systems infected with the worm might be programmed to establish destructive over/under pressure conditions by running 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	400	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.

Notes: Highlights compiled by CRS from the reports.

Table 7. International Efforts

Title	Source	Date	Pages	Notes
European Cybercrime Center (EC3)	Europol	Ongoing	N/A	The European Commission decided to establish a European Cybercrime Centre (EC3) at Europol. The centre will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. It will support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.
Global Cybersecurity Index	International Telecommunications Union	Ongoing	N/A	Based on questionnaire responses received by ITU Member States, a first analysis of cybersecurity development in the Arab region was compiled and one for the Africa region is under way. The objective is to release a global status of cybersecurity for 2014.
The Cyber Hub	Booz Allen Hamilton and the Economist Intelligence Unit	Ongoing	N/A	The Cyber Hub's content was built on several integral parts: an index that assesses specific aspects of the cyber environment of the G20 countries, and a series of research papers that examine the implications for the business community.
Cybersecurity Legislation	International Telecommunications Union	Ongoing	N/A	An integral and challenging component of any national Cybersecurity strategy is the adoption of regionally and internationally harmonized, appropriate legislation against the misuse of ICTs for criminal or other purposes.
Cyber Security Strategy: Progress So Far	UK Cabinet Office	Ongoing	N/A	From the report, "To support the Strategy we put in place a National Cyber Security Programme (NCSP) backed by £650 million of funding to 2015. This year we increased that investment with a further £210 million in 2015 to 2016. This funding will build on existing projects and also support new investment, enabling the UK to retain its emerging reputation as a leader in the field of cyber security."

Title	Source	Date	Pages	Notes
Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors	Senate Armed Services Committee	September 17, 2014	52	Hackers associated with the Chinese government successfully penetrated the computer systems of Transportation Command (TRANSCOM) contractors 20 times in the course of a single year. Chinese hackers tried to get into the systems 50 times. The congressional committee found that only two of the intrusions were detected. It also found the officials were unaware due in large part to unclear requirements and methods for contractors to report breaches and for government agencies to share information.
A Role for Civil Society in Cybersecurity Affairs?	ICT for Peace Foundation	September 3, 2014	26	"The paper is aimed at civil society organisations, national governments, international and regional organisations and other key actors concerned with ICTs and their impact on international and regional security. They perform a wide range of functions, including policy-oriented research, advocacy, [and] networking. In the Internet/ cyber security world, civil society organisations often work in specific issues areas, many technical or functional in nature and tied to the maintenance of the Internet. Civil society does not include the private sector. Nevertheless, natural alliances are emerging between certain of the more tech-oriented civil society organisations (for example, the Internet Society or the IEEE) and some Tier 1 carriers (i.e., those carriers that have a direct connection to the Internet and the networks it uses to deliver voice and data services), and major transnational vendors and Internet Service Providers (ISPs)."
Consult, Command, Control, Contract: Adding a Fourth "C" to NATO's Cyber Security	Centre for International Governance Innovation	August 6, 2014	10	The authors address the North Atlantic Treaty Organization to implement a contracting protocol that delineates appropriate classifications for the tasks and personnel required for private cyber-security contracts. They conclude that establishing an oversight organization and submitting a proposal to the International Law Commission to consider the roles of private security actors would create greater transparency and accountability for contracting.

Title	Source	Date	Pages	Notes
iDATA: Improving Defences Against Targeted Attack	Centre for the Protection of National Infrastructure (UK)	July 2014	8	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 a number of outputs for the cyber security community. This document provides a description of the iDATA program and a summary of the reports.
Cyber-attacks: Effects on UK	Oxford Economics	July 2014	79	The UK Centre for the Protection of National Infrastructure (CPNI) requested Oxford Economics to carry out a study of the impact of state-sponsored cyberattacks on UK firms. The study consists of the elaboration of an economic framework for cyberattacks, a survey of UK firms on cyberattacks, an event study on the impact of cyberattacks on stock market valuations, and a series of case studies illustrating the experience of several UK firms with cyberattacks.
Global Cybercrime: The Interplay of Politics and Law	Centre for International Governance Innovation (CIGI)	June 20, 2014	23	This paper explores the recent unsealing of a 31-count indictment against five Chinese government officials and a significant cyber breach, perpetrated by Chinese actors against Western oil, energy, and petrochemical companies. The paper concludes by noting that increased cooperation among governments is necessary, but unlikely to occur as long as the discourse surrounding cybercrime remains so heavily politicized and securitized. If governments coalesced around the notion of trying to prevent the long-term degradation of trust in the online economy, they may profitably advance the dialogue away from mutual suspicion and toward mutual cooperation.
China and International Law in Cyberspace	U.S.-China Economic and Security Review Commission	May 7, 2014	11	Despite major differences on cyberspace policy between the United States and China, a recent development at the United Nations illustrates basic areas of agreement. The United States and China were among 15 countries affirming the applicability of international law to cyberspace in a 2013 UN report. The same group will gather in 2014 to address some of the more challenging and divisive concepts regarding state responsibility and use of force in cyberspace.

Title	Source	Date	Pages	Notes
Baseline Review: ICT-Related Processes & Events, Implications for International and Regional Security (2011-2013)	ICT4Peace	May 1, 2014	50	The report is structured around the following three areas: (1) international and regional security (the predominant focus); (2) transnational crime and terrorism; and (3) governance, human rights and development. These areas are obviously interdependent, with developments in one area often impacting another, yet they have traditionally been approached separately through distinct communities of practice and fora. The report will serve as a baseline for future annual reports with this specific one covering the period spanning January 2011 to December 2013 (while also providing background on earlier events).
Cyber maturity in the Asia-Pacific Region 2014	Australian Strategic Policy Institute (ASPI)	April 14, 2014	76	The Institute assesses regional digital maturity across government, business, society and the military. Australia comes out ahead of China, Japan and South Korea when it comes to overall digital strength in the region and it ranks third behind the United States and China in cyber warfare. Asia-Pacific is increasingly the focus of cyberattacks, say analysts, including criminal and state-sponsored hacking and espionage.
U.S.-EU Cyber Cooperation	White House	March 26, 2014	N/A	The new high-level U.S.-EU Cyber Dialogue announced at the 2014 U.S.-EU Summit will formalize and broaden our cooperation on cyber issues, building on shared commitments and achievements in key areas.
Legislative resolution on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union	European Parliament	March 13, 2014	N/A	The directive would require companies operating critical infrastructure to maintain a specified minimum level of cybersecurity preparedness and report to national authorities about cyberattacks with a "significant impact" on the security of their networks.

Title	Source	Date	Pages	Notes
10 Steps to Cyber Security	UK Dept. for Business Innovation & Skills (BIS) and the Centre for the Protection of National Infrastructure (CPNI)	February 4, 2014	20	The joint communiqué outlines steps UK regulators and government departments have agreed to undertake to improve the country's cyber systems and networks defenses. The steps to combat cyberattacks include assessing the state of cybersecurity across each sector and working with industry to address vulnerabilities; working with industry to increase information flows on threat vulnerabilities and mitigation strategies; encouraging companies to join information sharing initiatives, such as the Cyber Security Information Sharing Partnership, a partnership between the U.K. government and industry to share information and intelligence on cybersecurity threats launched in March 2013; and encouraging companies to undertake a self-assessment pursuant to guidance published by the U.K. Department for Business, Innovation and Skills.
2013 Joint Report	U.S.-Russia Bilateral Presidential Commission (BPC)	December 27, 2013	40	The report includes updates from each of the BPC's 21 working groups. See the Working Group on the Threats to and in the use of Information Communications Technologies in the Context of International Service section on pages 11-12. A key component of the discussion concerned the implementation of the bilateral confidence building measures (CBMs) announced by Presidents Obama and Putin in June 2013. These bilateral CBMs are intended to promote transparency and reduce the possibility that an incident related to the use of ICTs could unintentionally cause instability or escalation.
World Federation of Exchanges (WFE) Launches Global Cyber Security Committee	World Federation of Exchanges	December 12, 2013	N/A	The WFE announced the launch of the exchange industry's first cybersecurity committee with a mission to aid in the protection of the global capital markets. The working group will bring together representation from a number of exchanges and clearinghouses across the globe, to collaborate on best practices in global security.

Title	Source	Date	Pages	Notes
Handbook on European Data Protection Law	Council of Europe	December 2013	214	This handbook is a first point of reference on both EU law and the European Convention on Human Rights (ECHR) on data protection, and it explains how this field is regulated under EU law and under the ECHR as well as the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and other CoE instruments. Each chapter first presents a single table of the applicable legal provisions, including important selected case law under the two separate European legal systems.
2013 Annual Report to Congress	U.S.-China Economic Commission	October 20, 2013	465	In 2013, the commission continued its close examination of China's cyber capabilities. Strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States, including the U.S. government and private companies. However, the public exposure of Chinese cyber espionage in 2013 has apparently not changed China's attitude about the use of cyber espionage to steal intellectual property and proprietary information. (See: Chapter 2, Section 2: "China's Cyber Activities.")
Directive of the European Parliament and of the Council on Attacks Against Information Systems	European Parliament Civil Liberties Committee	August 12, 2013	7	The objectives of the Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialized law enforcement services of the Member States, as well as the competent specialized Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).

Title	Source	Date	Pages	Notes
Confidence Building Measures and International Cybersecurity	ICT 4 Peace Foundation	June 21, 2013	21	Confidence building measures can serve to lay the foundation for agreeing on acceptable norms of behavior for states as well as confidence and trust building measures to avoid miscalculation and escalation. The report is divided into four main sections: (1) Transparency, Compliance, and Verification Measures; (2) Cooperative Measures; (3) Collaboration and Communication Mechanisms; and (4) Stability and Restraint Measures. A final section discusses next steps for diplomatic CBM processes.
FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security	White House	June 17, 2013	N/A	The United States and the Russian Federation are creating a new working group, under the auspices of the Bilateral Presidential Commission, dedicated to assessing emerging ICT threats and proposing concrete joint measures to address them.
Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment	Government Accountability Office	May 21, 2013	52	The federal government has begun efforts to address the security of the supply chain for commercial networks... There are a variety of other approaches for addressing the potential risks posed by foreign-manufactured equipment in commercial communications networks, including those approaches taken by foreign governments... While these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers, additional costs, and constraints on competition, which the federal government would have to take into account if it chose to pursue such approaches.
The Global Cyber Game: Achieving Strategic Resilience in the Global Knowledge Society	Defence Academy of the United Kingdom	May 8, 2013	127	Provides a systematic way of thinking about cyberpower and its use by a range of global players. The global cyberpower contest is framed as a Global Cyber Game, played out on a 'Cyber Gameboard'—a framework that can be used for strategic and tactical thinking about cyber strategy.

Title	Source	Date	Pages	Notes
Military and Security Developments Involving the People's Republic of China 2013 (Annual Report to Congress)	Department of Defense	May 6, 2013	92	China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high-technology industries, policy maker interest in U.S. leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis.
Defence White Paper 2013	Australia Department of Defence	May 3, 2013	148	The Australian Cyber Security Centre will bring together security capabilities from the Defence Signals Directorate, Defence Intelligence Organisation, Australian Security Intelligence Organisation (ASIO), the Attorney-General's Department's Computer Emergency Response Team (CERT) Australia, Australian Federal Police (AFP) and the Australian Crime Commission (ACC).
Remaking American Security: Supply Chain Vulnerabilities & National Security Risks Across the U.S. Defense Industrial Base	Alliance for American Manufacturing	May 2013	355	Because the supply chain is global, it makes sense for U.S. officials to cooperate with other nations to ward off cyberattacks. Increased international cooperation to secure the integrity of the global IT system is a valuable long-term objective.
Cyber Security Information Partnership (CISP)	Cabinet Office, United Kingdom	March 27, 2013	N/A	CISP introduces a secure virtual 'collaboration environment' where government and industry partners can exchange information on threats and vulnerabilities in real time. CISP will be complemented by a 'Fusion Cell,' which will be supported on the government side by the Security Service, GCHQ and the National Crime Agency, and by industry analysts from a variety of sectors.

Title	Source	Date	Pages	Notes
The Tallinn Manual on the International Law Applicable to Cyber Warfare	Cambridge University Press/ NATO Cooperative Cyber Defence Center of Excellence	March 5, 2013	302	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 each rules' 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 each rules' application. (Note: The manual is not an official NATO publication, but an expression of opinions of a group of independent experts acting solely in their personal capacity.)
APT1: Exposing One of China's Cyber Espionage Units	Mandiant	February 19, 2013	76	The details analyzed during hundreds of investigations signal that the groups conducting these activities (computer security breaches around the world) are based primarily in China and that the Chinese government is aware of them.
Worldwide Threat Assessment of the U.S. Intelligence Community (Testimony)	James Clapper, Director of National Intelligence	February 11, 2013	34	Clapper provided an assessment of global threats: U.S. critical infrastructure, eroding U.S. economic and national security, information control and Internet governance, and hactivists and criminals.
Linking Cybersecurity Policy and Performance	Microsoft Trustworthy Computing	February 6, 2013	27	Introduces a new methodology for examining how socio-economic factors in a country or region impact cybersecurity performance. Examines measures such as use of modern technology, mature processes, user education, law enforcement and public policies related to cyberspace. This methodology can build a model that will help predict the expected cybersecurity performance of a given country or region.
Comprehensive Study on Cybercrime	United Nations Office on Drugs and Crime (UNODC)	February 2013	320	The study examined the problem of cybercrime from the perspective of governments, the private sector, academia and international organizations. The results are presented in eight Chapters, covering Internet connectivity and cybercrime; the global cybercrime picture; cybercrime legislation and frameworks; criminalization of cybercrime; law enforcement and cybercrime investigations; electronic evidence and criminal justice; international cooperation in criminal matters involving cybercrime; and cybercrime prevention.

Title	Source	Date	Pages	Notes
Administration Strategy for Mitigating the Theft of U.S. Trade Secrets	White House	February 2013	141	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."
The Chinese Defense Economy Takes Off: Sector-by-Sector Assessments and the Role of Military End-Users	UC Institute on Global Conflict and Cooperation	January 25, 2013	87	This collection of 15 policy briefs explores how China has made such impressive military technological progress over the past few years, what is in store, and what are the international security implications. The briefs are summaries of a series of longer research papers presented at the third annual Chinese defense economy conference held by the Study of Innovation and Technology in China in July 2012.
Defence and Cyber-Security, vol. 1 - Report, together with formal minutes, oral and written evidence Defence and Cyber-Security, vol. 2 - Additional Written Evidence	House of Commons Defence Committee (UK)	December 18, 2012	99 (vol. 1) 37 (vol. 2)	Given the inevitable inadequacy of the measures available to protect against a constantly changing and evolving threat, and given the Minister for the Cabinet Office's comment, it is not enough for the Armed Forces to do their best to prevent an effective attack. In its response to this report the Government should set out details of the contingency plans it has in place should such an attack occur. If it has none, it should say so—and urgently create some.

Title	Source	Date	Pages	Notes
The Challenge of Cyber Power for Central African Countries: Risks and Opportunities	Naval Postgraduate School	December 2012	209	From the report,"The Central African militaries, which are supposed to be the first line of defense for their governments' institutions, are dramatically behind the times. To address this situation, the governments of Central Africa need to adopt a collaborative cyber strategy based on common investment in secure cyber infrastructures. Such cooperation will help to create a strong cyber environment conducive of the confidence and trust necessary for the emergence of a cyber community of Central African States (C3AS). For Central African militaries, massive training and recruiting will be the first move to begin the process of catching up."
Cybersecurity: Managing Risks for Greater Opportunities	Organization for Economic Co-operation and Development	November 29, 2012	N/A	The OECD launched a broad consultation of all stakeholders from member and non-member countries to review its Security Guidelines. The review takes into account newly emerging risks, technologies and policy trends around such areas as cloud computing, digital mobility, the Internet of things, social networking, etc.
Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy	Organization for Economic Co-operation and Development	November 16, 2012	117	This report analyzes the latest generation of national cybersecurity strategies in ten OECD countries and identifies commonalities and differences.
2012 Report to Congress of the U.S.-China Economic and Security Review Commission, One Hundred Twelfth Congress, Second Session, November 2012	U.S.-China Economic and Security Review Commission	November 2012	509	This report responds to the mandate for the commission "to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China." See "China's Cyber Activities," Chapter 2, Section 2, pp. 147-169.
Australia: Telecommunications Data Retention—an Overview	Parliamentary Library of Australia	October 24, 2012	32	In July 2012, the Commonwealth Attorney-General's Department released a Discussion Paper, Equipping Australia against emerging and evolving threats, on the proposed national security reforms.... Of the 18 primary proposals and the 41 individual reforms that they comprise, the suggestion that carriage service providers (CSPs) be required to routinely retain certain information associated with every Australian's use of the Internet and phone services for a period of up to two years ('data retention') is the issue that seems to have attracted the most attention.

Title	Source	Date	Pages	Notes
More Than Meets the Eye: Clandestine Funding, Cutting-Edge Technology and China's Cyber Research & Development Program	Lawrence Livermore National Laboratory	October 17, 2012	17	Analyzes how the Chinese leadership views information technology research and development (R&D), as well as the role cyber R&D plays in China's various strategic development plans. Explores the organizational structure of China's cyber R&D base. Concludes with a projection of how China might field new cyber capabilities for intelligence platforms, advanced weapons systems, and systems designed to support asymmetric warfare operations.
Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE	House Permanent Select Committee on Intelligence	October 8, 2012	60	The committee initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States.
Bilateral Discussions on Cooperation in Cybersecurity	China Institute of Contemporary International Relations and the Center for Strategic and International Studies (CSIS)	June 2012	N/A	Since 2009, CSIS and CICIR have held six formal meetings on cybersecurity (accompanied by several informal discussions), called "Sino-U.S. Cybersecurity Dialogue." The meetings have been attended by a broad range of U.S. and Chinese officials and scholars responsible for cybersecurity issues. The goals of the discussions have been to reduce misperceptions and to increase transparency of both countries' authorities and understanding on how each country approaches cybersecurity, and to identify areas of potential cooperation.
Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?	NATO	May 2012	8	In April 2007 a series of cyberattacks targeted Estonian information systems and telecommunication networks. Lasting 22 days, the attacks were directed at a range of servers (web, email, DNS) and routers. The 2007 attacks did not damage much of the Estonian information technology infrastructure. However, the attacks were a true wake-up call for NATO, offering a practical demonstration that cyberattacks could now cripple an entire nation dependent on IT networks.

Title	Source	Date	Pages	Notes
United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?	Triangle Institute for Security Studies	March 2012	34	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. Specifically, national CT cyber policies that are not completely sourced in domestic or international law unnecessarily limit the latitude cyber CT professionals need to effectively counter terrorists through the use of organic cyber capabilities. 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.
Cyber-security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness Around the World	McAfee	February 1, 2012	108	Forty-five percent of legislators and cybersecurity experts representing 27 countries think cybersecurity is just as important as border security. The authors surveyed 80 professionals from business, academia and government to gauge worldwide opinions of cybersecurity.
The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world	Cabinet Office (United Kingdom)	November 2011	43	Chapter 1 describes the background to the growth of the networked world and the immense social and economic benefits it is unlocking. Chapter 2 describes these threats. The impacts are already being felt and will grow as our reliance on cyberspace grows. Chapter 3 sets out where we want to end up—with the government's vision for UK cybersecurity in 2015.
Foreign Spies Stealing US Economic Secrets in Cyberspace	Office of the National Counterintelligence Executive	October 2011	31	According to the report, espionage and theft through cyberspace are growing threats to the United States' security and economic prosperity, and the world's most persistent perpetrators happen to also be U.S. allies.
International Strategy for Cyberspace	White House/OMB	May 16, 2011	30	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.
Cyber Dawn: Libya	Cyber Security Forum Initiative	May 9, 2011	70	Project Cyber Dawn: Libya uses open source material to provide an in-depth view of Libyan cyberwarfare capabilities and defenses.

Title	Source	Date	Pages	Notes
Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace	EastWest Institute	February 3, 2011	60	[The authors] led the cyber and traditional security experts through a point-by-point analysis of the Geneva and Hague Conventions. Ultimately, the group made five immediate recommendations for Russian and U.S.-led joint assessments, each exploring how to apply a key convention principle to cyberspace.
The Reliability of Global Undersea Communications Cable Infrastructure (The Rogucci Report)	IEEE/EastWest Institute	May 26, 2010	186	This study submits 12 major recommendations to the private sector, governments and other stakeholders—especially the financial sector—for the purpose of improving the reliability, robustness, resilience, and security of the world's undersea communications cable infrastructure.
German Anti-Botnet Initiative	Organisation for Economic Co-operation and Development (OECD)	December 8, 2009	4	This is a private industry initiative which aims to ensure that customers whose personal computers have become part of a botnet without them being aware of it are informed by their Internet Service Providers about this situation and at the same time are given competent support in removing the malware.

Note: Highlights compiled by CRS from the reports.

Table 8. Education/Training/Workforce

Title	Source	Date	Pages	Notes
NCCoE National Cybersecurity Excellence Partnerships	NIST National Cybersecurity Center of Excellence	Ongoing	N/A	Established in 2012 through a partnership between NIST, the state of Maryland, and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration, and adoption of practical cybersecurity solutions. The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division.
National Initiative for Cybersecurity Careers and Studies (NICCS)	Department of Homeland Security	Ongoing	N/A	NICCS is an online resource for cybersecurity career, education, and training information. It is a partnership between DHS, the National Institute of Standards and Technology, the Office of the Director of National Intelligence, the Department of Defense, the Department of Education, the National Science Foundation, and the Office of Personnel Management.
Experimental Research Testbed (DETER)	Department of Homeland Security	Ongoing	N/A	The DETER testbed is used to test and evaluate cybersecurity technologies by over 200 organizations from more than 20 states and 17 countries, including DHS-funded researchers, the larger cybersecurity research community, government, industry, academia, and educational users.
Michigan Cyber Range	Partnership between the state of Michigan, Merit Network, federal and local governments, colleges and universities, and the private sector	Ongoing	N/A	Enables individuals and organizations to develop detection and reaction skills through simulations and exercises.
Information Assurance Scholarship Program	Department of Defense	Ongoing	N/A	The Information Assurance Scholarship Program is designed to increase the number of qualified personnel entering the information assurance and information technology fields within the department. The scholarships also are an attempt to effectively retain military and civilian cybersecurity and IT personnel.

Title	Source	Date	Pages	Notes
National Centers of Academic Excellence (CAE) in Cyber Operations Program	National Security Agency (NSA)	Ongoing	N/A	The NSA has launched National Centers of Academic Excellence (CAE) in Cyber Operations Program; the program is intended to be a deeply technical, inter-disciplinary, higher education program grounded in the computer science (CS), computer engineering (CE), or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs and exercises.
Hackers Wanted: An Examination of the Cybersecurity Labor Market	RAND Corp.	June 24, 2014	110	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.
Cybersecurity for Government Contractorsnat	Robert Nichols et. al., West Briefing Papers	April 2014	28	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 begins with an overview of the most prevalent types of cyberattacks and targets, as well as the federal cybersecurity budget. Next, the paper outlines the current federal cybersecurity legal requirements applicable to government contractors, including statutory and regulatory requirements, the President's 2013 cybersecurity Executive Order (E.O.), and the resulting "cybersecurity framework" issued by the National Institute of Standards and Technology (NIST) in February 2014, as well as highlights further developments expected this year. Finally, it 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.

Title	Source	Date	Pages	Notes
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts	GAO	September 17, 2013	47	One in five jobs at a key cybersecurity component within DHS 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.
Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making	National Academies Press	September 16, 2013	66	This report examines workforce requirements for cybersecurity and 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.
Joint Professional Military Education Institutions in an Age of Cyber Threat	Francesca Spidalieri (Pell Center Fellow)	August 7, 2013	18	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. While these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists.
Special Cybersecurity Workforce Project (Memo for Heads of Executive Departments and Agencies)	Office of Personnel Management (OPM)	July 8, 2013	N/A	The OPM is collaborating with the White House Office of Science and Technology Policy, the Chief Human Capital Officers Council (CHCOC), and the Chief Information Officers Council (CIOC) 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 (EHRI) data warehouse by the end of FY2014.

Title	Source	Date	Pages	Notes
U.S.A. Cyber Warrior Scholarship Program	(ISC)² Foundation and Booz Allen Hamilton	June 21, 2013		The (ISC)² Foundation and Booz Allen Hamilton announced the launch of the U.S.A. Cyber Warrior Scholarship program, which will provide scholarships to veterans to obtain specialized certifications in the cybersecurity field. The scholarships will cover all of the expenses associated with a certification, such as training, textbooks, mobile study materials, certification testing, and the first year of certification maintenance fees.
Global Information Security Workforce Study	(ISC)² and Frost & Sullivan	May 7, 2013	28	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 and nearly three years of a continuing resolution.
Proposed Establishment of a Federally Funded Research and Development Center-First Notice	NIST	April 22, 2013	2	To help the National Cybersecurity Center of Excellence (NCCoE) address industry's needs most efficiently, NIST will sponsor its first Federally Funded Research and Development Center (FFRDC) to facilitate public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies.
DHS Secretary's Honors Program: Cyber Student Initiative	Department of Homeland Security	April 18, 2013	2	The Cyber Student Initiative program will begin at Immigration and Customs Enforcement computer forensic labs in 36 cities nationwide, where students will be trained and gain hands-on experience within the department's cybersecurity community. The unpaid volunteer program is only available to community college students and veterans pursuing a degree in the cybersecurity field.
2012 Information Technology Workforce Assessment for Cybersecurity	U.S. Department of Homeland Security	March 14, 2013	131	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 feds has more than 10 years of service until they reach retirement eligibility, nearly 33% will be eligible to retire in the next three years.
CyberSkills Task Force Report	U.S. Department of Homeland Security	October 2012	41	DHS's Task Force on CyberSkills proposes far-reaching improvements to enable DHS to recruit and retain the cybersecurity talent it needs.

Title	Source	Date	Pages	Notes
Cyber Security Test Bed: Summary and Evaluation Results	Institute for Homeland Security Solutions	October 2012	89	The Cyber Test Bed project was a case study analysis of how a set of interventions, including threat analysis, best practices sharing, and executive and staff training events, over the course of one year, would impact a group of nine small and mid-size businesses in North Carolina. Pre- and post-Test Bed interviews were conducted with company officials to establish a baseline and evaluate the impact of the Test Bed experience. After the Cyber Test Bed experience, decision makers at these companies indicated an increase in their perceptions of the risk of cyberattacks and an increase in their knowledge of possible solution.
Preparing the Pipeline: The U.S. Cyber Workforce for the Future	National Defense University	August 2012	17	This paper addresses methods to close the gaps between demand and the current existing capabilities and capacity in the U.S. cyber workforce. A large number of professionals with not only technical skills, but also an understanding of cyber policy, law, and other disciplines will be needed to ensure the continued success of the U.S. economy, government, and society in the 21st-century information age. Innovative methods have been developed by the government, think tanks, and private sector for closing these gaps, but more needs to be done.
Smart Grid Cybersecurity: Job Performance Model Report	Pacific Northwest National Laboratory	August 2012	178	This report outlines the work done to develop a smart grid cybersecurity certification. The primary purpose is to develop a measurement model that may be used to guide curriculum, assessments, and other development of technical and operational smart grid cybersecurity knowledge, skills, and abilities.

Title	Source	Date	Pages	Notes
Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination	Government Accountability Office (GAO)	November 29, 2011	86	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 Secretary of Commerce, Director of the Office of Management and Budget, Director of the Office of Personnel Management, and Secretary of Homeland Security should collaborate through the National Initiative for Cybersecurity Education (NICE) linitiative to develop and finalize detailed plans allowing agency accountability, measurement of progress, and determination of resources to accomplish agreed-upon activities.
NICE Cybersecurity Workforce Framework	National Initiative for Cybersecurity Education (NICE)	November 21, 2011	35	The adoption of cloud computing into the federal government and its implementation depend upon a variety of technical and non-technical 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. This document presents the NIST Cloud Computing Reference Architecture (RA) and Taxonomy (Tax) that will accurately communicate the components and offerings of cloud computing.
The State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States	National Cyber Security Alliance and Microsoft	May 2011	16	This year's survey further explores the perceptions and practices of U.S. teachers, school administrators and technology coordinators in regards to cyberethics, cybersafety, and cybersecurity education. The survey finds that young people still are not receiving adequate training and that teachers are ill-prepared to teach the subjects due, in large part, to lack of professional development.

Title	Source	Date	Pages	Notes
Cyber Operations Personnel Report	Department of Defense	April 2011	84	This report is focused on FY2009 Department of Defense Cyber Operations personnel, with duties and responsibilities as defined in Section 934 of the Fiscal Year (FY) 2010 National Defense Authorization Act (NDAA). 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
The Power of People: Building an Integrated National Security Professional System for the 21st Century	Project on National Security Reform (PNSR)	November 2010	326	This study was conducted in fulfillment of Section 1054 of the *National Defense Authorization Act for Fiscal Year 2010*, 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."

Note: Highlights compiled by CRS from the reports.

Table 9. Research & Development (R&D)

Title	Source	Date	Pages	Notes
Cyber Consortium	Fortinet and Palo Alto Networks	Ongoing	N/A	The consortium will seek to share intelligence on threats across large security vendors and aid a coordinated response to incidents. No customer data will be shared, only malware samples. The pair of companies also extend an open invitation to other security firms to join them, provided they can share at least 1,000 samples of new malware executables each day.
National Cybersecurity Center of Excellence (NCCoE)	National Institute of Standards and Technology (NIST)	Ongoing	N/A	The National Cybersecurity Center of Excellence (NCCoE) is a new public-private collaboration to bring together experts from industry, government and academia to design, implement, test, and demonstrate integrated cybersecurity solutions and promote their widespread adoption.
Policies for Enhancing U.S. Leadership in Cyberspace	National Science Foundation	August 20, 2014	N/A	This project focuses on three areas where U.S. policy could provide additional leadership in cyberspace: publication of zero-day exploits; labeling of neutral infrastructure, such as networks associated with hospitals or religious sites, and shared norms to protect neutral cyberspaces; and sustainment of Internet interoperability, which allows Internet users on different networks to communicate directly without interference. The findings may benefit national security by giving policy makers a way of assessing the costs and benefits of publishing exploits or patches.
Third-Party Security Assurance Information Supplement	PCI Security Standards Council	August 7, 2014	N/A	The Payment Card Industry Security Standards Council has created guidelines meant to help banks and merchants mitigate the risks posed by third parties that process credit card payment information. The guidance by the Payment Card Industry Security Standards Council includes practical recommendations on how to conduct due diligence and risk assessment when engaging third-party service providers to help organizations understand the services provided.

Title	Source	Date	Pages	Notes
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	13	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/exaggerate the risk of re-identification. While the research does raise important issues concerning the use of proper de-identification techniques, it does not suggest that de-identification should be abandoned.
Software Defined Perimeter Working Group	Cloud Security Alliance	December 1, 2013	13	This document explains the software defined perimeter (SDP) security framework and how it can be deployed to protect application infrastructure from network-based attacks. The SDP incorporates security standards from organizations such as NIST as well as security concepts from organizations such as DOD into an integrated framework.
DARPA Announces Cyber Grand Challenge	Defense Advanced Research Projects Agency (DARPA)	October 23, 2013	N/A	DARPA intends to hold the Cyber Grand Challenge (CGC)—the first-ever tournament for fully automatic network defense systems. The Challenge will see teams creating automated systems that would compete against each other to evaluate software, test for vulnerabilities, generate security patches, and apply them to protected computers on a network. The winning team in the CGC finals would receive a cash prize of $2 million, with second place earning $1 million and third place taking home $750,000.
Resilience metrics for cyber systems (free registration required to download)	Seager, Thomas (Arizona State University)	November 2013	6	Despite the national and international importance, resilience metrics to inform management decisions are still in the early stages of development. The resilience matrix framework developed by Linkov et al. is applied to develop and organize effective resilience metrics for cyber systems. These metrics link national policy goals to specific system measures, such that resource allocation decisions can be translated into actionable interventions and investments. The paper proposes a generic approach and could integrate actual data, technical judgment, and literature-based measures to assess system resilience across physical, information, cognitive, and social domains.

Title	Source	Date	Pages	Notes
Cybersecurity Exercise: Quantum Dawn 2	SIFMA	October 21, 2013	N/A	Quantum Dawn 2 is a cybersecurity exercise to test incident response, resolution, and coordination processes for the financial services sector and the individual member firms to a street-wide cyberattack.
Proposed Establishment of a Federally Funded Research and Development Center—Second Notice	National Institute of Standards and Technology	June 21, 2013	2	NIST intends to sponsor an FFRDC to facilitate public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. This is the second of three notices that must be published over a 90-day period to advise the public of the agency's intention to sponsor an FFRDC.
Governor McDonnell Announces Creation of MACH37, America's Premier Market-Centric Cyber Security Accelerator	Virginia Secretary of Commerce and Trade	April 11, 2013	N/A	Virginia Governor Bob McDonnell announced the creation of MACH37, a cybersecurity accelerator to be located at the Center for Innovative Technology. Initially funded by the Commonwealth of Virginia, the accelerator will leverage private investments to launch new, high growth cyber technology companies in Virginia.
Open Trusted Technology Provider Standard (O-TTPS)™, Version 1.0: Mitigating Maliciously Tainted and Counterfeit Products	The Open Group	April 2013	44	Specifically intended to prevent maliciously tainted and counterfeit products from entering the supply chain, this first release of the O-TTPS codifies best practices across the entire COTS ICT product lifecycle, including the design, sourcing, build, fulfillment, distribution, sustainment, and disposal phases. The O-TTPS will enable organizations to implement best practice requirements and allow all providers, component suppliers, and integrators to obtain Trusted Technology Provider status. (Registration required.)
The International Cyber-Security Ecosystem (video lecture)	Anthony M. Rutkowski, Distinguished Senior Research Fellow at the Georgia Institute of Technology, Nunn School Center for International Strategy Technology and Policy (CISTP)	November 6, 2012	N/A	Overview of the various forums/communities and methodologies that comprise the security assurance ecosystem—often also referred to as Information Assurance.
20 Critical Security Controls for Effective Cyber Defense	Center for Strategic & International Studies	November 2012	89	The Top 20 security controls were agreed upon by a consortium. Members of the Consortium include NSA, US CERT, DOD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DOD Cyber Crime Center plus commercial forensics experts in the banking and critical infrastructure communities.

Title	Source	Date	Pages	Notes
SBIR Phase II: Information Security Risk Taking	National Science Foundation (NSF)	January 17, 2012	N/A	The NSF is funding research on giving organizations information-security risk ratings, similar to credit ratings for individuals.
Anomaly Detection at Multiple Scales (ADAMS)	Defense Advanced Research Projects Agency (DARPA)	November 9, 2011	74	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.
At the Forefront of Cyber Security Research	NSF	August 5, 2011	N/A	TRUST is a university and industry consortium that examines cybersecurity issues related to health care, national infrastructures, law and other issues facing the general public.
Designing A Digital Future: Federally Funded Research And Development In Networking And Information Technology	White House	December 2010	148	The President's Council of Advisors on Science and Technology (PCAST) has made several recommendations in a report about the state of the government's Networking and Information Technology Research and Development (NITRD) Program.
Partnership for Cybersecurity Innovation	White House Office of Science and Technology Policy	December 6, 2010	10	The Obama Administration released a Memorandum of Understanding (below) signed by the National Institute of Standards and Technology of the Department of Commerce, the Science and Technology Directorate of the Department of Homeland Security (DHS/S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our nation's critical infrastructures.
Memorandum of Understanding (MOU)	NIST, DHS, and Financial Services Sector Coordinating Council	December 2, 2010	4	The document formalizes the intent of the parties 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.
Science of Cyber-Security	Mitre Corp (JASON Program Office)	November 2010	86	JASON was requested by DOD to examine the theory and practice of cyber-security, and evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach, identify what is needed in creating a science of cyber-security, and recommend specific ways in which scientific methods can be applied.
American Security Challenge: Moving Innovation to Market	National Security Initiative	October 18, 2010	N/A	The objective of the Challenge is to increase the visibility of innovative technology and help the commercialization process so that such technology can reach either the public or commercial marketplace faster to protect our citizens and critical assets.

Note: Highlights compiled by CRS from the reports.

Selected Reports, by Federal Agency

This section contains selected cybersecurity reports from U.S. government agencies, including the White House, the Office of Management and Budget (OMB), the Government Accountability Office (GAO), the Department of Defense (DOD), the National Institute of Standards and Technology (NIST), and others.

Table 10. Government Accountability Office (GAO)

Title	Date	Pages	Notes
Healthcare.gov: Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses	September 18, 2014	17	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 implemented by the Centers for Medicare & Medicaid Services (CMS) to protect the security and privacy of the information and IT systems supporting Healthcare.gov. While CMS has security and privacy-related protections in place for Healthcare.gov and related systems, weaknesses exist that put these systems and the sensitive personal information they contain at risk.
Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls	September 16, 2014	78	GAO is making six recommendations to implement security and privacy management controls to help ensure that the systems and information related to Healthcare.gov are protected. HHS concurred but disagreed in part with GAO's assessment of the facts for three recommendations. However, GAO continues to believe its recommendations are valid, as discussed in the report.
Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts	September 15, 2014	82	Homeland Security (DHS) used 10 different assessment tools and methods from fiscal 2011 through 2013 to assess critical infrastructure vulnerabilities. Four of the 10 assessments did not include cybersecurity. The differences in the assessment tools and methods mean DHS is not positioned to integrate its findings in identifying priorities.
Information Security: Agencies Need to Improve Oversight of Contractor Controls	September 8, 2014	43	Although the six federal agencies that GAO reviewed (the Departments of Energy (DOE), DHS, State, and Transportation (DOT), the Environmental Protection Agency (EPA), and the Office of Personnel Management (OPM)) generally established security and privacy requirements and planned for assessments to determine the effectiveness 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. The following table shows the degree of implementation of oversight activities at selected agencies.

Title	Date	Pages	Notes
FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain	July 17, 2014	30	The Federal Deposit Insurance Corporation (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. During 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.
Information Security: Additional Oversight Needed to Improve Programs at Small Agencies	June 25, 2014	54	The six small agencies GAO reviewed have made mixed progress in implementing elements of information security and privacy programs as required by the Federal Information Security Management Act of 2002, the Privacy Act of 1974, the E-Government Act of 2002, and Office of Management and Budget (OMB) guidance. In a separate report for limited official use only, GAO is providing specific details on the weaknesses in the six selected agencies' implementation of information security and privacy requirements.
Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity	June 5, 2014	54	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.
Information Security: Agencies Need to Improve Cyber Incident Response Practices	April 30, 2014	55	Twenty-four major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information). Based on a statistical sample of cyber incidents reported in fiscal year 2012, GAO projects that these agencies did not completely document actions taken in response to detected incidents in about 65% of cases.
Information Security: SEC Needs to Improve Controls over Financial Systems and Data	April 17, 2014	25	Although the SEC had implemented and made progress in strengthening information security controls, weaknesses limited their effectiveness in protecting the confidentiality, integrity, and availability of a key financial system. Until SEC mitigates control deficiencies and strengthens the implementation of its security program, its financial information and systems may be exposed to unauthorized disclosure, modification, use, and disruption. These weaknesses, considered collectively, contributed to GAO's determination that SEC had a significant deficiency in internal control over financial reporting for FY2013.

Title	Date	Pages	Notes
IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk	April 8, 2014	29	Until the 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, were the basis of our determination that IRS had a significant deficiency in its internal control over its financial reporting systems for FY2013.
Federal Agencies Need to Enhance Responses to Data Breaches	April 2, 2014	19	Major federal agencies continue to face challenges in fully implementing all components of an agency-wide information security program, which is essential for securing agency systems and the information they contain—including personally identifiable information (PII).
Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology	January 27, 2013	41	GAO was asked to review federal coordination with state and local governments regarding cybersecurity at public safety entities. The objective was to determine the extent to which federal agencies coordinated with state and local governments regarding cybersecurity efforts at emergency operations centers, public safety answering points, and first responder organizations involved in handling 911 emergency calls. To do so, GAO analyzed relevant plans and reports and interviewed officials at (1) five agencies that were identified based on their roles and responsibilities established in federal law, policy, and plans and (2) selected industry associations and state and local governments.
Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent	December 9, 2013	67	GAO recommends, "Recommendation: 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, 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."
GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced	November 6, 2013	58	GAO was asked to review the effects of 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 DOT [Department of Transportation] 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.

Title	Date	Pages	Notes
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts	September 17, 2013	47	One in five jobs at a key cybersecurity component within DHS 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.
Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment	May 21, 2013	52	The federal government has begun efforts to address the security of the supply chain for commercial networks... There are a variety of other approaches for addressing the potential risks posed by foreign-manufactured equipment in commercial communications networks, including those approaches taken by foreign governments... Although these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers, additional costs, and constraints on competition, which the federal government would have to take into account if it chose to pursue such approaches.
Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts	April 11, 2013	45	Until the Department of Homeland Security 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. While no cyber incidents have been reported affecting the nation's core and access networks, communications networks operators can use reporting mechanisms established by FCC and DHS to share information on outages and incidents.
Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities	April 4, 2013	72	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 Departments of Justice (DOJ) and 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 entities working together and sharing information is important, but they do not hold the entities accountable for such coordination.
Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges	March 7, 2013	36	"[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 DHS.... [I]t remains unclear how OMB and DHS are to share oversight of individual departments and agencies. Additional legislation could clarify these responsibilities."

Title	Date	Pages	Notes
2013 High Risk List	February 14, 2013	275	Every two years at the start of a new Congress, GAO calls attention to 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. Cybersecurity programs on the list include: *Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures* and *Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests*.
Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented	February 14, 2013	112	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.
Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project	January 25, 2013	35	"The 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 components of the ESN project as of August 2012 resulted in unnecessary risk that sensitive information could be disclosed, modified, or obtained without authorization. GAO is making seven recommendations to the FCC to implement management controls to help ensure that ESN meets its objective of securing FCC's systems and information."
Cybersecurity: Challenges in Securing the Electricity Grid	July 17, 2012	25	In a prior report, GAO has made recommendations related to electricity grid modernization efforts, including developing an approach to monitor compliance with voluntary standards. These recommendations have not yet been implemented.
Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned	July 11, 2012	43	To help ensure the success of agencies' implementation of cloud-based solutions, 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 officer (CIO) to establish estimated costs, performance goals, and plans to retire associated legacy systems for each cloud-based service discussed in this report, as applicable.
Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight	July 9, 2012	46	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.

Title	Date	Pages	Notes
Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage	June 28, 2012	20	This 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 IP.
Cybersecurity: Challenges to Securing the Modernized Electricity Grid	February 28, 2012	19	As GAO reported in January 2011, securing smart grid systems and networks presented a number of key challenges that required attention by government and industry. GAO made several recommendations to the Federal Energy Regulatory Commission (FERC) aimed at addressing these challenges. The commission agreed with these recommendations and described steps it is taking to implement them.
Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use	December 9, 2011	77	Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.
Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination	November 29, 2011	86	All the agencies GAO reviewed faced challenges determining the size of their cybersecurity workforce because of variations in how work is defined and the lack of an occupational series specific to cybersecurity. With respect to other workforce planning practices, all agencies had defined roles and responsibilities for their cybersecurity workforce, but these roles did not always align with guidelines issued by the federal Chief Information Officers Council (CIOC) and National Institute of Standards and Technology (NIST).
Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management	October 17, 2011	72	GAO is recommending that OMB update its guidance to establish measures of accountability for ensuring that CIOs' responsibilities are fully implemented and require agencies to establish internal processes for documenting lessons learned.
Information Security: Additional Guidance Needed to Address Cloud Computing Concerns	October 5, 2011	17	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.
Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements	October 3, 2011	49	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 over 650% over the past 5 years. Each of the 24 agencies reviewed had weaknesses in information security controls.

Title	Date	Pages	Notes
Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management	October 17, 2011	72	GAO is recommending that the Office of Management and Budget (OMB) update its guidance to establish measures of accountability for ensuring that CIOs' responsibilities are fully implemented and require agencies to establish internal processes for documenting lessons learned.
Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates	July 29, 2011	33	This letter discusses the Department of Defense's cyber and information assurance budget for FY2012 and future years defense spending. The objectives of this review 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.
Continued Attention Needed to Protect Our Nation's Critical Infrastructure	July 26, 2011	20	A number of significant challenges remain to enhancing the security of cyber-reliant critical infrastructures, such as (1) implementing actions recommended by the President's cybersecurity policy review; (2) updating the national strategy for securing the information and communications infrastructure; (3) reassessing DHS's planning approach to critical infrastructure protection; (4) strengthening public-private partnerships, particularly for information sharing; (5) enhancing the national capability for cyber warning and analysis; (6) addressing global aspects of cybersecurity and governance; and (7) securing the modernized electricity grid.
Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities	July 25, 2011	79	GAO recommends that DOD evaluate how it is organized to address cybersecurity threats; assess the extent to which it has developed joint doctrine that addresses cyberspace operations; examine how it assigned command and control responsibilities; and determine how it identifies and acts to mitigate key capability gaps involving cyberspace operations.
Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain	July 8, 2011	63	The Department of State implemented a custom application called iPost and a risk scoring program that is intended to provide continuous monitoring capabilities of information security risk to elements of its information technology (IT) infrastructure. To improve implementation of iPost at State, the Secretary of State should direct the Chief Information Officer to develop, document, and maintain an iPost configuration management and test process.
Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems	March 16, 2011	16	Executive branch agencies have made progress instituting several government-wide initiatives aimed at bolstering aspects of federal cybersecurity, such as reducing the number of federal access points to the Internet, establishing security configurations for desktop computers, and enhancing situational awareness of cyber events. Despite these efforts, the federal government continues to face significant challenges in protecting the nation's cyber-reliant critical infrastructure and federal information systems.

Title	Date	Pages	Notes
Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed	January 12, 2011	50	GAO identified six key challenges: (1) Aspects of the regulatory environment may make it difficult to ensure smart grid systems' cybersecurity. (2) Utilities are focusing on regulatory compliance instead of comprehensive security. (3) The electric industry does not have an effective mechanism for sharing information on cybersecurity. (4) Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems. (5) There is a lack of security features being built into certain smart grid systems. (6) The electricity industry does not have metrics for evaluating cybersecurity.
Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk	November 30, 2010	50	Existing government-wide guidelines and oversight efforts do not fully address agency implementation of leading wireless security practices. Until agencies take steps to better implement these leading practices, and OMB takes steps to improve government-wide oversight, wireless networks will remain at an increased vulnerability to attack.
Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed	October 6, 2010	66	Of the 24 recommendations in the President's May 2009 cyber policy review report, 2 have been fully implemented, and 22 have been partially implemented. While these efforts appear 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.
DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened	September 23, 2010	46	The Department of Homeland Security (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.
Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems	September 15, 2010	38	OMB and NIST established policies and guidance for civilian non-national security systems, while 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 was asked to assess the progress of federal efforts to harmonize policies and guidance for these two types of systems.
United States Faces Challenges in Addressing Global Cybersecurity and Governance	August 2, 2010	53	GAO recommends that the Special Assistant to the President and Cybersecurity Coordinator should make recommendations to appropriate agencies and interagency coordination committees regarding any necessary changes to more effectively coordinate and forge a coherent national approach to cyberspace policy.

Title	Date	Pages	Notes
Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed	July 15, 2010	38	The Special Assistant to the President and Cybersecurity Coordinator and the Secretary of Homeland Security should take two actions: (1) use the results of this report to focus their information-sharing efforts, including their relevant pilot projects, on the most desired services, including providing timely and actionable threat and alert information, access to sensitive or classified information, a secure mechanism for sharing information, and security clearance and (2) bolster the efforts to build out the National Cybersecurity and Communications Integration Center as the central focal point for leveraging and integrating the capabilities of the private sector, civilian government, law enforcement, the military, and the intelligence community.
Federal Guidance Needed to Address Control Issues With Implementing Cloud Computing	July 1, 2010	53	To assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing, the Director of OMB should establish milestones for completing a strategy for implementing the federal cloud computing initiative.
Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats	June 16, 2010	15	Multiple opportunities exist to improve federal cybersecurity. To address identified deficiencies in agencies' security controls and shortfalls in their information security programs, GAO and agency inspectors general 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. While 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.
Information Security: Concerted Response Needed to Resolve Persistent Weaknesses	March 24, 2010	21	Without proper safeguards, federal computer systems are vulnerable to intrusions by individuals who have malicious intentions and can obtain sensitive information. The need for a vigilant approach to information security has been 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.
Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats	March 16, 2010	15	The White House, the Office of Management and Budget, and certain federal agencies have undertaken several government-wide initiatives intended to enhance information security at federal agencies. While 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.

Title	Date	Pages	Notes
Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies	April 12, 2010	40	To reduce the threat to federal systems and operations posed by cyberattacks on the United States, OMB launched, in November 2007, the Trusted Internet Connections (TIC) initiative, and later, in 2008, DHS's National Cybersecurity Protection System (NCPS), operationally known as Einstein, which became mandatory for federal agencies as part of TIC. To further ensure that federal agencies have adequate, sufficient, and timely information to successfully meet the goals and objectives of the TIC and Einstein programs, DHS's Secretary should, to better understand whether Einstein alerts are valid, develop additional performance measures that indicate how agencies respond to alerts.
Cybersecurity: Progress Made But Challenges Remain in Defining and Coordinating the Comprehensive National Initiative	March 5, 2010	64	To address strategic challenges in areas that are not the subject of existing projects within CNCI but remain key to achieving the initiative's overall goal of securing federal information systems, OMB's Director should continue developing a strategic approach to identity management and authentication, linked to HSPD-12 implementation, as initially described in the CIOC's plan for implementing federal identity, credential, and access management, so as to provide greater assurance that only authorized individuals and entities can gain access to federal information systems.
Continued Efforts Are Needed to Protect Information Systems from Evolving Threats	November 17, 2009	24	GAO has 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; and log, audit, and monitor security-relevant events, among other actions.
Efforts to Improve Information sharing Need to Be Strengthened	August 27, 2003	59	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.
Computer Attacks at Department of Defense Pose Increasing Risk	May 1996	48	DISA estimates indicate that Defense may have been attacked as many as 250,000 times last year. 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 Defense systems 65 percent of the time.

Source: Highlights compiled by CRS from the GAO reports.

Table 11. White House/Office of Management and Budget[2]

Title	Date	Pages	Notes
Improving Cybersecurity	Ongoing	N/A	OMB is working with agencies, Inspectors General, Chief Information Officers, senior agency officials in charge of privacy, as well as 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.
Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices	October 3, 2014	17	OMB is making these updates to streamline agency reporting of information security incidents to the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT), and to improve DHS US-CERT's ability to respond to information security incidents effectively... Losses of personally identifiable information caused by non-electronic means still need reporting within an hour of a confirmed breach, but to the agency privacy office rather than US-CERT.
Federal Information Security Management Act, Annual Report to Congress	May 1, 2014	80	The 24 largest federal departments and agencies spent $10.34 billion on cybersecurity last fiscal year. The CFO Act agency with the greatest expenditure was Defense, at $7.11 billion, followed by Homeland Security 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.
Assessing Cybersecurity Regulations	May 22, 2014	N/A	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 NSIT 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.
Big Data: Seizing Opportunities, Preserving Values	May 2014	85	The findings outline a set of consumer protection recommendations, including that Congress should pass legislation on "single national data breach standard."

[2] For a list of White House executive orders, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.

Title	Date	Pages	Notes
State and Local Government Cybersecurity	April 2, 2014	N/A	The White House in March 2014 convened a broad 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	December 12, 2013	308	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."
Immediate Opportunities for Strengthening the Nation's Cybersecurity	November 2013	31	This is a report of the President's Council of Advisors on Science and Technology (PCAST). The report recommends the government phase out insecure, outdated operating systems, like Windows XP, implement better encryption technology, and encourage automatic security updates, among other changes. PCAST also recommends, for regulated industries, that the government help create cybersecurity best practices and audit their adoption—and for independent agencies, PCAST write new rules that require businesses to report their cyber improvements.
Cross Agency Priority Goal: Cybersecurity, FY2013 Q3 Status Report	October 2013	24	Executive branch departments and agencies will achieve 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.
Incentives to Support Adoption of the Cybersecurity Framework	August 6, 2013	N/A	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."

Title	Date	Pages	Notes
FY2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002	March 2013	68	More government programs violated data security law standards in 2012 than in the previous year, and 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 FISMA adherence scores 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.
Administration Strategy for Mitigating the Theft of U.S. Trade Secrets	February 20, 2013	141	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."
National Strategy for Information Sharing and Safeguarding	December 2012	24	Provides guidance for effective development, integration, and implementation of policies, processes, standards, and technologies to promote secure and responsible information sharing.
Collaborative and Cross-Cutting Approaches to Cybersecurity	August 1, 2012	N/A	Michael Daniel, White House Cybersecurity Coordinator, highlights a few recent initiatives where voluntary, cooperative actions are helping to improve the nation's overall cybersecurity.
Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program	December 2011	36	As a research and development strategy, this plan defines four strategic thrusts: Inducing Change, Developing Scientific Foundations, Maximizing Research Impact, and Accelerating Transition to Practice.
FY2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management	September 14, 2011	29	Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate re-authorization process is not necessary.
Cybersecurity Legislative Proposal (Fact Sheet)	May 12, 2011	N/A	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.

Title	Date	Pages	Notes
International Strategy for Cyberspace	May 2011	30	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.
National Strategy for Trusted Identities in Cyberspace (NSTIC)	April 15, 2011	52	The NSTIC aims to make online transactions more trustworthy, thereby giving businesses and consumers more confidence in conducting business online.
Federal Cloud Computing Strategy	February 13, 2011	43	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.
25 Point Implementation Plan to Reform Federal Information Technology Management	December 9, 2010	40	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.
Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security	July 6, 2010	39	This memorandum outlines and clarifies the respective responsibilities and activities of the Office of Management and Budget (OMB), the Cybersecurity Coordinator, and DHS, in particular with respect to the Federal Government's implementation of the Federal Information Security Management Act of 2002 (FISMA).
The National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy (Draft)	June 25, 2010	39	The NSTIC, which is in response to one of the near-term action items in the President's Cyberspace Policy Review, calls for the creation of an online environment, or an Identity Ecosystem, where individuals and organizations can complete online transactions with confidence, trusting the identities of each other and the identities of the infrastructure where transaction occur.
Comprehensive National Cybersecurity Initiative (CNCI)	March 2, 2010	5	The CNCI establishes a multi-pronged 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.

Title	Date	Pages	Notes
Cyberspace Policy Review: Assuring a Trusted and Resilient Communications Infrastructure	May 29, 2009	76	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. This 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.

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

Table 12. Department of Defense (DOD)

Title	Source	Date	Pages	Notes
Program Protection and System Security Engineering Initiative	DOD Systems Engineering	Ongoing	N/A	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, the 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.
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	234	The purpose of this paper is to assist DOD program managers and their staffs in making effective software assurance and software supply chain risk management decisions. This paper also describes some key gaps that were identified in the course of this 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.
Risk Management Framework (RMF) for DOD Information Technology (IT)	Department of Defense	March 12, 2014	47	In a change in security policy, DOD has dropped its long-standing DOD Information Assurance Certification and Accreditation Process (DIACAP) and adopted a risk-focused security approach developed by the National Institute of Standards and Technology (NIST). The decision, issued in a DOD Instruction memo (8510.01), aligns for the first time the standards the Defense Department and civilian agencies use to ensure their IT systems comply with approved information assurance and risk management controls.
Improving Cybersecurity and Resilience through Acquisition	Department of Defense and the General Services Administration (GSA)	January 23, 2014	24	The 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.

Title	Source	Date	Pages	Notes
Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information	DOD	November 18, 2013	10	The final rule imposed two new requirements. First, the rule imposed an obligation on contractors to provide "adequate security" to safeguard "unclassified controlled technical information" (UCTI). Second, contractors are obligated 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." UCTI should be marked with a DOD "distribution statement." This is the first time that the DOD has imposed specific requirements for cybersecurity that are generally applicable to all contractors.
Offensive Cyber Capabilities at the Operational Level - The Way Ahead	Center for Strategic & International Studies (CSIS)	September 16, 2013	20	The specific question this report examines is whether the Defense Department should make a more deliberate effort to explore the potential of offensive cyber tools at levels below that of a combatant command.
An Assessment of the Department of Defense Strategy for Operating in Cyberspace	U.S. Army War College	September 2013	60	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*. In the second part, each strategic initiative is elaborated and critiqued in terms of significance, novelty, and practicality. In the third part, the monograph critiques the DOD Strategy as a whole.
Joint Professional Military Education Institutions in an Age of Cyber Threat	Francesca Spidalieri (Pell Center Fellow)	August 7, 2013	18	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. While these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists.

Title	Source	Date	Pages	Notes
Military and Security Developments Involving the People's Republic of China 2013 (Annual Report to Congress)	DOD	May 6, 2013	92	China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high-technology industries, policy maker interest in U.S. leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis.
Resilient Military Systems and the Advanced Cyber Threat	DOD Science Board	January 2013	146	The report states that, despite numerous Pentagon actions to parry sophisticated attacks by other countries, efforts are "fragmented" and the Defense Department "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.
FY2012 Annual Report	DOD	January 2013	372	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.
Basic Safeguarding of Contractor Information Systems (Proposed Rule)	DOD, GSA, and National Aeronautics and Space Administration (NASA)	August 24, 2012	4	This regulation authored by the 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)."
Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight	GAO	July 9, 2012	46	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.

Title	Source	Date	Pages	Notes
Cloud Computing Strategy	DOD, Chief Information Officer	July 2012	44	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.
DOD Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities	*Federal Register*	May 11, 2012	7	DOD interim final rule to establish a voluntary cybersecurity information sharing program between DOD and eligible DIB companies. The program enhances and supplements DIB participants' capabilities to safeguard DOD information that resides on, or transits, DIB unclassified information.
DOD Information Security Program: Overview, Classification, and Declassification	DOD	February 24, 2012	84	Describes the DOD Information Security Program, and provides guidance for classification and declassification of DOD information that requires protection in the interest of the national security.
Cyber Sentries: Preparing Defenders to Win in a Contested Domain	Air War College	February 7, 2012	38	This 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 the department to operate effectively in the contested cyber domain in accordance with the vision established in its Strategy for Cyberspace Operations.
Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates	GAO	July 29, 2011	33	This letter discusses DOD's cyber and information assurance budget for FY2012 and future years defense spending. The objectives of this review 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.
Legal Reviews of Weapons and Cyber Capabilities	Secretary of the Air Force	July 27, 2011	7	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" must undergo legal review—except for cyber capabilities within a Special Access Program, which must undergo review by the Air Force general counsel.

Title	Source	Date	Pages	Notes
Department of Defense Strategy for Operating in Cyberspace	DOD	July 2011	19	This is an unclassified summary of DOD's cyber-security strategy.
Cyber Operations Personnel Report (DOD)	DOD	April 2011	84	This report focuses on FY2009 Department of Defense Cyber Operations personnel, with duties and responsibilities as defined in Section 934 of the Fiscal Year 2010 National Defense Authorization Act (NDAA). 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
Anomaly Detection at Multiple Scales (ADAMS)	Defense Advanced Research Projects Agency (DARPA)	November 9, 2011	74	The design document was produced by Allure Security and sponsored by the Defense Advanced Research Projects Agency (DARPA). It 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.
Critical Code: Software Producibility for Defense	National Research Council, Committee for Advancing Software-Intensive Systems Producibility	October 20, 2010	160	Assesses the nature of the national investment in software research and, in particular, considers ways to revitalize the knowledge base needed to design, produce, and employ software-intensive systems for tomorrow's defense needs.
Defending a New Domain	U.S. Deputy Secretary of Defense, William J. Lynn (Foreign Affairs)	September/October 2010	N/A	In 2008, DOD suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. This previously classified incident was the most significant breach of U.S. military computers ever, and served as an important wake-up call.
The QDR in Perspective: Meeting America's National Security Needs In the 21st Century (QDR Final Report)	Quadrennial Defense Review	July 30, 2010	159	From the report: "The expanding cyber mission also needs to be examined. DOD should be prepared to assist civil authorities in defending cyberspace – beyond the department's current role."
Cyberspace Operations: Air Force Doctrine Document 3-12	U.S. Air Force	July 15, 2010	62	This Air Force Doctrine Document (AFDD) establishes doctrinal guidance for the employment of U.S. Air Force operations in, through, and from cyberspace. It is the keystone of Air Force operational-level doctrine for cyberspace operations.

Title	Source	Date	Pages	Notes
DON (Department of the Navy) Cybersecurity/Information Assurance Workforce Management, Oversight and Compliance	U.S. Navy	June 17, 2010	14	To establish policy and assign responsibilities for the administration of the Department of the Navy (DON) Cybersecurity (CS)/Information Assurance Workforce (IAWF) Management Oversight and Compliance Program.

Note: Highlights compiled by CRS from the reports.

CRS Product: Cybersecurity Framework

- CRS Report WSLG829, *National Institute of Standards and Technology Issues Long-awaited Cybersecurity Framework*, by Andrew Nolan

Table 13. National Institute of Standards and Technology (NIST)

Including the Cybersecurity Framework

Title	Date	Pages	Notes
Computer Security Division, Computer Security Resource Center	Ongoing	N/A	Compilation of laws, regulations, and directives from 2000-2007 that govern the creation and implementation of federal information security practices. These laws and regulations provide an infrastructure for overseeing implementation of required practices, and charge NIST with developing and issuing standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.
NIST/NCCoE Establishment of a Federally Funded Research and Development Center	September 22, 2014	N/A	The Mitre Corp. will run NIST's cybersecurity Federally Funded Research and Development Center on a contract worth up to $5 billion over five years. Mitre already operates six individual FFRDCs for agencies including the Defense Department and Federal Aviation Administration. It's also active in cybersecurity, for example managing the Common Vulnerabilities and Exposures database — which catalogues software security flaws. It also developed specifications for the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) under contract from DHS.
Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems	May 13, 2014	121	NIST has 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 has released the first set of those guidelines for public comment in a new draft document.

Title	Date	Pages	Notes
Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (SP 800-52r1)	April 28, 2014	67	The federal government must upgrade its servers to handle version 1.1 of Transportation Layer Security and make plans by January 2015 for handling web traffic encrypted using TLS 1.2. TLS is a common method of encrypting web traffic and email that relies on public key encryption. The Internet Engineering Task Force approved TLS 1.2 in August 2008, but it is only recently that browsers have begun to support it.
National Cybersecurity Center of Excellence (NCCoE) and Electric Power Sector Identity and Access Management Use Case	March 18, 2014	2	NIST invites organizations to provide products and technical expertise to support and demonstrate security platforms for identity and access management for the electric power sector. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the Energy Sector program. Participation in the use case is open to all interested organizations.
Framework for Improving Critical Infrastructure Cybersecurity	February 12, 2014	41	The voluntary framework consists of cybersecurity standards that can be customized to various sectors and adapted by both large and small organizations. Additionally, so that the private sector may fully adopt this Framework, the Department of Homeland Security announced the Critical Infrastructure Cyber Community (C^3)—or "C-cubed"—Voluntary Program. The C^3 program gives companies that provide critical services like cell phones, email, banking, energy, and state and local governments, direct access to cybersecurity experts within DHS who have knowledge about specific threats, ways to counter those threats, and how, over the long term, to design and build systems that are less vulnerable to cyber threats.
Update on the Development of the Cybersecurity Framework	January 15, 2014	3	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."
Proposed Establishment of a Federally Funded Research and Development Center	January 10, 2014	2	NIST intends to sponsor a Federally Funded Research and Development Center (FFRDC) to facilitate public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. NIST published three notices in the *Federal Register* advising the public of the agency's intention to sponsor an FFRDC and requesting comments from the public. This notice provides NIST's analysis of the comments related to NIST's proposed establishment of the FFRDC received in response to those notices.
Designed-in Cyber Security for Cyber-Physical Systems	November 20, 2013	60	NIST and the Cybersecurity Research Alliance held a two-day workshop (April 4-5, 2013) for industry, government, and academic cybersecurity researchers. The report's findings lay out a logical roadmap for designing security into varied IP-based systems and platforms increasingly targeted by cyber attackers.

Title	Date	Pages	Notes
Cybersecurity Framework	October 22, 2013	47	NIST seeks comments on the preliminary version of the Cybersecurity Framework ("preliminary Framework"). Under Executive Order 13636, NIST is directed to work with stakeholders to develop a framework to reduce cyber risks to critical infrastructure.
A Role-Based Model for Federal Information Technology/Cybersecurity Training (Draft Special Publication 800-16 Revision 1)	October 2013	152	This guidance will assist managers at all level to understand their responsibilities in providing role-based cybersecurity training,
Guide to Attribute Based Access Control Definition and Considerations (Draft SP 800-162)	October 2013	48	Improving information sharing while maintaining control over access to that information is a primary goal of guidance coming from the NIST.
Discussion Draft of the Preliminary Cybersecurity Framework	August 28, 2013	36	The Framework provides a common language and mechanism for organizations to (1) describe current cybersecurity posture; (2) describe their target state for cybersecurity; (3) identify and prioritize opportunities for improvement within the context of risk management; (4) assess progress toward the target state; (5) foster communications among internal and external stakeholders.
Proposed Establishment of a Federally Funded Research and Development Center-Third Notice	July 16, 2013	2	This is the third of three notices that must be published over a 90-day period to advise the public of the agency's intention to sponsor an FFRDC.
DRAFT Outline—Preliminary Framework to Reduce Cyber Risks to Critical Infrastructure	July 1, 2013	5	This draft is produced for discussion purposes at the upcoming workshops and to further encourage private-sector input before NIST publishes a preliminary Draft *Framework to Reduce Cyber Risks to Critical Infrastructure* ("the Framework") for public comment in October.
Computer Security Incident Coordination (CSIC): Providing Timely Cyber Incident Response	June 28, 2013	3	NIST is seeking information relating to Computer Security Incident Coordination (CSIC) as part of the research needed to write a NIST Special Publication (SP) to help Computer Security Incident Response Teams (CSIRTs) coordinate effectively when responding to computer-security incidents. The NIST SP will identify technical standards, methodologies, procedures, and processes that facilitate prompt and effective response.
Proposed Establishment of a Federally Funded Research and Development Center—Second Notice	June 21, 2013	2	NIST intends to sponsor an FFRDC to facilitate public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. This is the second of three notices that must be published over a 90-day period to advise the public of the agency's intention to sponsor an FFRDC.
Update on the Development of the Cybersecurity Framework	June 18, 2013	3	NIST is seeking input about foundational cybersecurity practices, ideas for how to manage privacy and civil liberties needs, and outcome-oriented metrics that leaders can use in evaluating the position and progress of their organizations' cybersecurity status. In a few weeks, NIST expects to post an outline of the preliminary cybersecurity framework, including existing standards and practices.

Title	Date	Pages	Notes
Initial Analysis of Cybersecurity Framework RFI Responses	May 15, 2013	34	NIST released an initial analysis of 243 responses to the Feb. 26 RFI. The analysis will form the basis for an upcoming workshop at Carnegie Mellon University in Pittsburgh as NIST moves forward on creating a cybersecurity framework for essential energy, utility and communications systems.
Proposed Establishment of a Federally Funded Research and Development Center-First Notice	April 22, 2013	2	To help the National Cybersecurity Center of Excellence (NCCoE) address industry's needs most efficiently, NIST will sponsor its first FFRDC to facilitate public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies.
Security and Privacy Controls for Federal Information Systems (SP 800-53, Rev. 4)	April 2013	457	Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing 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.
Developing a Framework To Improve Critical Infrastructure Cybersecurity, Notice; Request for Information	February 26, 2013	5	NIST announced the first step in the development of a Cybersecurity Framework, which will be a set of voluntary standards and best practices to guide industry in reducing cyber risks to the networks and computers that are vital to the nation's economy, security, and daily life.
Memorandum of Understanding (MOU)	December 2, 2010	4	The MOU, signed by NIST, DHS, and the Financial Services Sector Coordinating Council (FSSCC), formalizes the intent of the parties 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.

Note: Highlights compiled by CRS from the reports.

Table 14. Other Federal Agencies

Title	Source	Date	Pages	Notes
Office of Cybersecurity and Communications (CS&C)	DHS	Ongoing	N/A	CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C 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	Ongoing	N/A	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.
Cybersecurity Collection	The National Academies Press	Ongoing	N/A	The prevention of cyberattacks on a nation's important computer and communications system and networks is a problem that looms large. In order to best prevent such attacks, this collection explains the importance of increasing the usability of security technologies, recommends strategies for future research aimed at countering cyberattacks, and considers how information technology systems can be used to not only maximize protection against attacks, but also respond to threats.
Federal Incident Reporting Guidelines	US-CERT	October 1, 2014	10	The guidance tells federal agencies to classify incidents according to their impacts, rather than by categories of attack methods. It also modifies a 2007 requirement for agencies to report to US-CERT within an hour any incident involving the loss of personally identifiable information. Rather, agencies should notify US-CERT of 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 said in a concurrently-released memo that losses of personally identifiable information caused by non-electronic means still need reporting within an hour of a confirmed breach, but to the agency privacy office rather than US-CERT.

Title	Source	Date	Pages	Notes
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	FDA	October 1, 2014	9	The guidance, first issued as a draft in June 2013, tells manufactures to "develop a set of cybersecurity controls." It also tells manufactures to consider following the core functions of the NIST cybersecurity framework — a model for cybersecurity activities: Identify, Protect, Detect, Respond, and Recover.
Collaborative Approaches for Medical Device and Healthcare Cybersecurity; Public Workshop; Request for Comments	Food and Drug Administration	September 23, 2014	3	The FDA announced an Oct. 21-22 workshop on collaborative approaches for medical device and health-care cybersecurity. FDA, in collaboration with other stakeholders within the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS), seeks broad input from the Healthcare and Public Health (HPH) Sector on medical device and healthcare cybersecurity. The vision for this public workshop is to catalyze collaboration among all HPH stakeholders.
Health Insurance Marketplaces Generally Protected Personally Identifiable Information but Could Improve Certain Information Security Controls	DHS Office of Inspector General	September 22, 2014	N/A	The websites and databases in some state health insurance exchanges are still vulnerable to attack, putting personally identifiable information (PII) at risk. The report examined the website and databases of the federal insurance exchange, as well as the state exchanges for Kentucky and New Mexico
Energy Sector Cybersecurity Framework Implementation Guidance - Draft For Public Comment & Comment Submission Form	DOE Office of Electricity Delivery and Energy Reliability	September 12, 2014	N/A	Energy companies need not make a choice between the NIST cybersecurity framework and the DOE's Cybersecurity Capability Maturity Model. The NIST framework tells organizations to grade themselves on a four-tier scale based on their overall cybersecurity program sophistication. C2M2 tells users to assess cybersecurity control implementation across 10 "domains" of cybersecurity practices such as "situational awareness" according to their specific "maturity indicator level."
Implementation Status of the Enhanced Cybersecurity Services Program	DHS Office of Inspector General	July 2014	23	The National Protection Programs Directorate (NPPD) has made progress in expanding the Enhanced Cybersecurity Services program. For example, as of May 2014, 40 critical infrastructure entities participate in the program. Additionally, 22 companies have signed memorandums of agreement to join the program. Although NPPD has made progress, the Enhanced Cybersecurity Services program has been slow to expand because of limited outreach and resources. In addition, cyber threat information sharing relies on NPPD's manual reviews and analysis, which has led to inconsistent cyber threat indicator quality.

Title	Source	Date	Pages	Notes
At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues	National Academies Press	May 13, 2014	102	The report is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.
HHS activities to enhance cybersecurity	Department of Health and Human Services	May 12, 2014	N/A	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," the HHS report concluded. "Expanding any or each of these authorities solely to address cybersecurity issues would not be appropriate or recommended."
Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)	Department of Justice	May 9, 2014	7	The Department of Justice 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 whitepaper says that the law does not prohibit companies from divulging data in the aggregate, without any specific details about identifiable customers.
Inadequate Practice and Management Hinder Department's Incident Detection and Response	Department of Commerce Office of Inspector General	April 24, 2014	15	Auditors sent a prolonged stream of deliberately suspicious network traffic to five public-facing websites at the department—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.

Title	Source	Date	Pages	Notes
OCIE Cybersecurity Initiative	SEC	April 15, 2014	9	The SEC's Office of Compliance Inspections and Examinations (OCIE) will be conducting examinations of more than 50 registered broker-dealers and registered investment advisers, focusing on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.
Antitrust Policy Statement on Sharing of Cybersecurity Information	Department of Justice and Federal Trade Commission	April 10, 2014	9	Information-sharing about cyberthreats can be done lawfully as long as companies aren't 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 cyberthreat information," said Deputy Attorney General James Cole. "Antitrust concerns should not get in the way of sharing cybersecurity information."
Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition	General Services Administration and Department of Defense	March 12, 2014	1	On January 23, 2014, the GSA and DOD posted the Final Report of the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition on the DOD and GSA websites. The report makes six recommendations to improve cybersecurity and resilience in federal acquisitions. This Request for Comments is being published to obtain stakeholder input on how to implement the report's recommendations.
High-Risk Security Vulnerabilities Identified During Reviews of Information Technology General Controls at State Medicaid Agencies	Department of Health and Human Services, Office of Inspector General	March 2014	20	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.
Self-Regulatory Organizations; Chicago Board Options Exchange, Incorporated; Notice of Withdrawal of Proposed Rule Change Relating to Multi-Class Spread Orders	Securities and Exchange Commission	February 24, 2014	1	The SEC is soliciting comments on proposed amendments to the Financial Industry Regulatory Authority's (FINRA's) arbitration codes to ensure that parties' private information, such as Social Security and financial account numbers, are redacted to include only the last four digits of the number. The proposed amendments would apply only to documents filed with FINRA. They would not apply to documents that parties exchange with each other or submit to the arbitrators at a hearing on the merits.

Title	Source	Date	Pages	Notes
SEC to Hold Cybersecurity Roundtable	Securities and Exchange Commission	February 14, 2014	N/A	The SEC announced that it will host a roundtable to discuss cybersecurity, the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns. The roundtable will be held at the SEC's Washington, DC, headquarters on March 26 and will be open to the public and webcast live on the SEC's website. Information on the agenda and participants will be published in the coming weeks.
The Critical Infrastructure Cyber Community C³ Voluntary Program	DHS	February 12, 2014	N/A	The C³ Voluntary Program will serve as a point of contact and customer relationship manager to assist organizations with Framework use and guide interested organizations and sectors to DHS and other public and private-sector resources to support use of the Cybersecurity Framework.
The Federal Government's Track Record on Cybersecurity and Critical Infrastructure	Sen. Homeland Security and Governmental Affairs Committee (Minority Staff)	February 4, 2013	19	Since 2006, the federal government has spent at least $65 billion on securing its computers and networks, according to an estimate by the Congressional Research Service. NIST, the government's official body for setting cybersecurity standards, has produced thousands of pages of precise guidance on every significant aspect of IT security. And yet agencies—even agencies with responsibilities for critical infrastructure, or vast repositories of sensitive data—continue to leave themselves vulnerable, often by failing to take the most basic steps towards securing their systems and information.
Improving Cybersecurity and Resilience through Acquisition	General Services Administration (GSA) and the Department of Defense	January 23, 2014	24	The 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.
The Department of Energy's July 2013 Cyber Security Breach	DOE Inspector General	December 2013	28	The report states nearly eight times as many current and former Energy Department staff members were affected by a July 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.

Title	Source	Date	Pages	Notes
Improving Cybersecurity and Resilience through Acquisition	General Services Administration and Department of Defense	January 23, 2014	24	The 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.
Evaluation of DHS' Information Security Program for Fiscal Year 2013	DHS Inspector General	November 2013	50	The report reiterates that the agency uses outdated security controls and Internet connections that are not verified as trustworthy, as well as for not reviewing its "top secret" information systems for vulnerabilities.
Immediate Opportunities for Strengthening the Nation's Cybersecurity	President's Council of Advisors on Science and Technology (PCAST)	November 2013	31	The report recommends the government phase out insecure, outdated operating systems, like Windows XP, implement better encryption technology, and encourage automatic security updates, among other changes. PCAST also recommends, for regulated industries, that the government help create cybersecurity best practices and audit their adoption—and for independent agencies, PCAST write new rules that require businesses to report their cyber improvements.
Federal Energy Regulatory Commission's Unclassified Cyber Security Program - 2013	Department of Energy Office of Inspector General	October 2013	13	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 to FY2012... As directed by FISMA, the Office of Inspector General conducted an independent evaluation of the Commission's unclassified cybersecurity program to determine whether it adequately protected data and information systems. This report presents the results of our evaluation for FY2013.

Title	Source	Date	Pages	Notes
DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Center	DHS Inspector General	October 2013	29	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, or the NCCIC, is tasked with sharing information about malicious activities on government networks with cybersecurity offices within the Defense Department, the FBI and federal intelligence agencies. But the DHS center and the five federal cybersecurity hubs do not all have the same technology or resources, preventing them from having shared situational awareness of intrusions or threats and restricting their ability to coordinate response. The centers also have not created a standard set of categories for reporting incidents.
Special Cybersecurity Workforce Project (Memo for Heads of Executive Departments and Agencies)	Office of Personnel Management (OPM)	July 8, 2013	N/A	The OPM is collaborating with the White House Office of Science and Technology Policy, the Chief Human Capital Officers Council (CHCOC), and the Chief Information Officers Council (CIOC) 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 (EHRI) data warehouse by the end of FY2014.
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Notice	Food and Drug Administration (FDA)	June 14, 2013	1	This guidance identifies cybersecurity issues that manufacturers should consider in preparing premarket submissions for medical devices to maintain information confidentiality, integrity, and availability.
DHS Can Take Actions to Address Its Additional Cybersecurity Responsibilities	Department of Homeland Security	June 2013	26	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 actions have been taken, NPPD can make further improvements to address its additional cybersecurity responsibilities.
Mobile Security Reference Architecture	Federal CIO Council and the Department of Homeland Security (DHS)	May 23, 2013	103	Gives agencies guidance in the secure implementation of mobile solutions through their enterprise architectures. The document provides in-depth reference architecture for mobile computing.

Title	Source	Date	Pages	Notes
Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E^3A)	Department of Homeland Security	April 19, 2013	27	DHS will deploy EINSTEIN 3 Accelerated (E3A) to enhance cybersecurity analysis, situational awareness, and security response. Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks. This Privacy Impact Assessment (PIA) is being conducted because E3A will include analysis of federal network traffic, which may contain personally identifiable information (PII).
DHS Secretary's Honors Program: Cyber Student Initiative	Department of Homeland Security	April 18, 2013	2	The Cyber Student Initiative program will begin at Immigration and Customs Enforcement computer forensic labs in 36 cities nationwide, where students will be trained and will gain hands-on experience within the department's cybersecurity community. The unpaid volunteer program is only available to community college students and veterans pursuing a degree in the cybersecurity field.
Regulation Systems Compliance and Integrity	Securities and Exchange Commission	March 25, 2013	104	The SEC is examining the exposure of stock exchanges, brokerages, and other Wall Street firms to cyberattacks. The proposed rule asks whether stock exchanges should be required to tell members about breaches of critical systems. More than half of exchanges surveyed globally in 2012 said they experienced a cyberattack, while 67% of U.S. exchanges said a hacker tried to penetrate their systems.
National Level Exercise 2012: Quick Look Report	Federal Emergency Management Agency	March 2013	22	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. As a part of the National Exercise Program, NLE 2012 emphasized the shared responsibility among all levels of government, the private sector, and the international community to secure cyber networks and coordinate response and recovery actions. The NLE 2012 series was 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.

Title	Source	Date	Pages	Notes
Measuring What Matters: Reducing Risks by Rethinking How We Evaluate Cybersecurity	National Academy of Public Administration and Safegov.org	March 2013	39	Rather than periodically auditing whether an agency's systems meet the standards enumerated in Federal Information Security Management Act (FISMA) at a static moment in time, agencies and their inspectors general should keep running scorecards of "cyber risk indicators" based on continual IG assessments of a federal organization's cyber vulnerabilities.
Follow-up Audit of the Department's Cyber Security Incident Management Program	Department of Energy Inspector General	December 2012	25	"In 2008, we reported in The Department's Cyber Security Incident Management Program (DOE/IG-0787, January 2008) that the Department and NNSA established and maintained a number of independent, at least partially duplicative, cyber security incident management capabilities. Although certain actions had been taken in response to our prior report, we identified several issues that limited the efficiency and effectiveness of the Department's cyber security incident management program and adversely impacted the ability of law enforcement to investigate incidents. For instance, we noted that the Department and NNSA continued to operate independent, partially duplicative cyber security incident management capabilities at an annual cost of more than $30 million. The issues identified were due, in part, to the lack of a unified, Department-wide cyber security incident management strategy. In response to our finding, management concurred with the recommendations and indicated that it had initiated actions to address the issues identified."
Secure and Trustworthy Cyberspace (SaTC) Program Solicitation	National Science Foundation and the National Science and Technology Council (NSTC)	October 4, 2012	N/A	This grant program seeks proposals that address Cybersecurity from a Trustworthy Computing Systems perspective (TWC); a Social, Behavioral and Economic Sciences perspective (SBE); and a Transition to Practice perspective (TPP).
Annual Report to Congress 2012: National Security Through Responsible Information Sharing	Information Sharing Environment (ISE)	June 30, 2012	188	From the report, "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."

Title	Source	Date	Pages	Notes
Cybersecurity: CF Disclosure Guidance: Topic No. 2	Securities and Exchange Commission	October 13, 2011	N/A	The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the commission has neither approved nor disapproved its content.

Note: Highlights compiled by CRS from the reports.

Table 15. State, Local and Tribal Governments

Title	Source	Date	Pages	Notes
Getting Started for State, Local, Tribal, and Territorial (SLTT) Governments	US-CERT	Ongoing	N/A	The resources listed are available to state, local, tribal, and territorial governments. These resources have been aligned to the five Cybersecurity Framework Function Areas. Some resources and programs align to more than one Function Area. This page will be updated as additional resources—from DHS, other federal agencies, and the private sector—are identified.
State Governments at Risk: Time to Move Forward: 2014 Deloitte-NASCIO Cybersecurity Study	Deloitte & Touche and National Association of State CIOs	October 2014	32	A majority of elected officials in state governments are confident in their abilities to defend against cyberthreats, but only one-quarter of state CISOs feel the same way, according to a new survey. In the survey of 49 state CISOs or their equivalents and 186 other state officials, barriers to cybersecurity that were cited included low budgets and difficulty recruiting top talent. Three-quarters of the CISOs said lack of sufficient funding is a major barrier to addressing cyberthreats, though almost half said cybersecurity budgets have increased year over year.
Cybersecurity and Connecticut's Public Utilities	Connecticut Public Utilities Regulatory Authority	April 14, 2014	31	The document is a plan for Connecticut's utilities to help strengthen defense against possible future threats, such as a cyberattack. Connecticut is the first state to present a cybersecurity strategy in partnership with the utilities, and will share it with other states working on similar plans. Among other findings, the report recommends that Connecticut commence self-regulated cyber audits and reports, and move toward a third-party audit and assessment system. The report also makes recommendations regarding local and regional regulatory roles, emergency drills and training, coordinating with emergency management officials, and handling confidential information.

Title	Source	Date	Pages	Notes
State and Local Government Cybersecurity	White House Blog	April 2, 2014	N/A	The White House in March 2014 convened a broad 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.
State Cybersecurity Resource Guide: Awareness, Education and Training Initiatives	National Association of State Chief Information Officers	October 2013	64	The guide includes new information from our state members, who provided examples of state awareness programs and initiatives. This is an additional resource of best-practice information, together with an interactive state map to allow users to drill-down to the actual resources that states have developed or are using to promote cyber awareness. It includes contact information for the CISO [Chief Information Officers], hyperlinks to state security and security awareness pages, and information describing cybersecurity awareness, training, and education initiatives.
Cybersecurity for State Regulators 2.0 with Sample Questions for Regulators to Ask Utilities	National Association of Regulatory Utility Commissioners	February 2013	31	State commissions tasked with regulating local distribution utilities are slow to respond to emerging cybersecurity risks. The annual membership directory of state utility regulators lists hundreds of key staff members of state commissions throughout the country, but not a single staff position had "cybersecurity" in the title.
Federal Support for and Involvement in State and Local Fusion Centers	U.S. Senate Permanent Subcommittee on Investigations	October 3, 2012	141	A two-year bipartisan investigation found that U.S. Department of Homeland Security 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.

Notes: Highlights compiled by CRS from the reports.

Related Resources: Other Websites

This section contains other cybersecurity resources, including U.S. government, international, news sources, and other associations and institutions.

Table 16. Related Resources: Congressional/Government

Name	Source	Notes
Integrated Intelligence Center (IIC)	Center for Internet Security	Serves as a resource for state, local, tribal, and territorial government partners to engage in a collaborative information sharing and analysis environment on cybersecurity issues. Through this initiative the IIC provides fusion centers, homeland security advisors, and law enforcement entities with access to a broad range of cybersecurity products, reflecting input from many sources.
Computer Security Resource Center	National Institute of Standards and Technology (NIST)	Links to NIST resources, publications, and computer security groups.
Congressional Cybersecurity Caucus	Led by Representatives Jim Langevin and Mike McCaul.	Provides statistics, news on congressional cyberspace actions, and links to other information websites.
Cybersecurity	White House National Security Council	Links to White House policy statements, key documents, videos, and blog posts.
Cybersecurity	National Telecommunications & Information Administration (U.S. Department of Commerce)	The Department of Commerce's Internet Policy Task Force is conducting a comprehensive review of the nexus between cybersecurity challenges in the commercial sector and innovation in the Internet economy.
Cybersecurity and Information System Trustworthiness	National Academy of Sciences, Computer Science and Telecommunications Board	A list of CSTB's independent and informed reports on cybersecurity and public policy.
Getting Started for State, Local, Tribal, and Territorial (SLTT) Governments	U.S. CERT	The resources are available to state, local, tribal, and territorial governments. These resources have been aligned to the five Cybersecurity Framework Function Areas. Some resources and programs align to more than one Function Area. This page will be updated as additional resources—from DHS, other federal agencies, and the private sector—are identified.
President's National Security Telecommunications Advisory Committee (NSTAC)	U.S. Department of Homeland Security	NSTAC's goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis and to help the U.S. government maintain a reliable, secure, and resilient national communications posture.

Name	Source	Notes
Office of Cybersecurity and Communications (CS&C)	U.S. Department of Homeland Security	CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C 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
Cyber Domain Security and Operations	U.S. Department of Defense	Links to press releases, fact sheets, speeches, announcements, and videos.
U.S. Cyber-Consequences Unit	U.S. Cyber-Consequences Unit (U.S.-CCU)	U.S.-CCU, a nonprofit 501c(3) research institute, provides assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks. It also investigates the likelihood of such attacks and examines the cost-effectiveness of possible counter-measures.

Note: Highlights compiled by CRS from the reports.

Table 17. Related Resources: International Organizations

Name	Source	Notes
Center for Internet Security (Australia)	Australian Communications and Media Authority	The Australian Internet Security Initiative (AISI) is an antibotnet initiative that collects data on botnets in collaboration with Internet Service Providers (ISPs), and two industry codes of practice.
Cybercrime	Council of Europe	Links to the Convention on Cybercrime treaty, standards, news, and related information.
Cybersecurity Gateway	International Telecommunications Union (ITU)	ITU's Cybersecurity Gateway aims to be a collaborative platform, providing and sharing information between partners in civil society, private sector, governmental and international organizations working in different work areas of cybersecurity
Cybercrime Legislation - Country Profiles	Council of Europe	These profiles have been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation.
ENISA: Securing Europe's Information Society	European Network and Information Security Agency (ENISA)	ENISA inform businesses and citizens in the European Union on cybersecurity threats, vulnerabilities, and attacks. (Requires free registration to access.)
International Cyber Security Protection Alliance (ICSPA)	International Cyber Security Protection Alliance (ICSPA)	A global not-for-profit organization that aims to channel funding, expertise, and help directly to law enforcement cyber-crime units around the world.
NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) (Tallin, Estonia)	North Atlantic Treaty Organization (NATO)	The Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, the Slovak Republic, and Spain as sponsoring nations, to enhance NATO's cyber-defence capability.

Note: Highlights compiled by CRS from the reports.

Table 18. Related Resources: News

Name	Source
Computer Security (Cybersecurity)	*New York Times*
Cybersecurity	NextGov.com
Cyberwarfare and Cybersecurity	Benton Foundation
Homeland Security	Congressional Quarterly (CQ)
Cybersecurity	Homeland Security News Wire

Table 19. Related Resources: Other Associations and Institutions

Name	Notes
Council on Cybersecurity	The Council, based in the Washington, DC, area, is the successor organization to the National Board of Information Security Examiners (NBISE), founded in the United States in 2010 to identify and strengthen the skills needed to improve the performance of the cybersecurity workforce. The Council will also be home to the U.S. Cyber Challenge, (formerly a program of NBISE), that works with the cybersecurity community to bring accessible, compelling programs that motivate students and professionals to pursue education, development, and career opportunities in cybersecurity.
Cyber Aces Foundation	Offers challenging and realistic cybersecurity competitions, training camps, and educational initiatives through which high school, college students, and young professionals develop the practical skills needed to excel as cybersecurity practitioners.
Cybersecurity from the Center for Strategic & International Studies (CSIS)	Links to experts, programs, publications, and multimedia. CSIS is a bipartisan, nonprofit organization whose affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change.
Cyberconflict and Cybersecurity Initiative from the Council on Foreign Relations	Focuses on the relationship between cyberwar and the existing laws of war and conflict; how the United States should engage other states and international actors in pursuit of its interests in cyberspace; how the promotion of the free flow of information interacts with the pursuit of cybersecurity; and the private sector's role in defense, deterrence, and resilience.

Name	Notes
Cyber Corps: Scholarship For Service (SFS)	Scholarship For Service (SFS) is designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning.
Institute for Information Infrastructure Protection (I3P)	I3P is a consortium of leading universities, national laboratories and nonprofit institutions. I3P assembles multi-disciplinary and multi-institutional research teams able to bring in-depth analysis to complex and pressing problems. Research outcomes are shared at I3P-sponsored workshops, professional conferences and in peer-reviewed journals, as well as via technology transfer to end-users.
Internet Security Alliance (ISA)	ISAalliance is a nonprofit collaboration between the Electronic Industries Alliance (EIA), a federation of trade associations, and Carnegie Mellon University's CyLab.
National Association of State Chief Information Officers (NASCIO)	NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. The Resource Guide provides examples of state awareness programs and initiatives.
National Initiative for Cybersecurity Education (NICE)	The goal of NICE is to establish an operational, sustainable, and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. NIST is leading the NICE initiative, including more than 20 federal departments and agencies, to ensure coordination, cooperation, focus, public engagement, technology transfer, and sustainability.
National Security Cyberspace Institute (NSCI)	NSCI provides education, research and analysis services to government, industry, and academic clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities.
U.S. Cyber Challenge (USCC)	USCC's goal is to find 10,000 of America's best and brightest to fill the ranks of cybersecurity professionals where their skills can be of the greatest value to the nation.

Source: Highlights compiled by CRS from the reports of related associations and institutions.

Author Contact Information

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

Key Policy Staff

The following table provides names and contact information for CRS experts on policy issues related to cybersecurity bills currently being debated in the 113th Congress.

Legislative Issues	Name/Title	Phone	Email
Legislation in the 113th Congress	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Critical infrastructure protection	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Chemical industry	Dana Shea	7-6844	dshea@crs.loc.gov
Defense industrial base	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Electricity grid	Richard J. Campbell	7-7905	rcampbell@crs.loc.gov
Financial institutions	N. Eric Weiss	7-6209	eweiss@crs.loc.gov
Industrial control systems	Dana Shea	7-6844	dshea@crs.loc.gov
Cybercrime			
Federal laws	Charles Doyle	7-6968	cdoyle@crs.loc.gov
Law enforcement	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
Cybersecurity workforce	Wendy Ginsberg	7-3933	wginsberg@crs.loc.gov
Cyberterrorism	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Cyberwar	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Data breach notification	Gina Stevens	7-2581	gstevens@crs.loc.gov
Economic issues	N. Eric Weiss	7-6209	eweiss@crs.loc.gov
Espionage			
Advanced persistent threat	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Economic and industrial	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
Legal issues	Brian T. Yeh	7-5182	byeh@crs.loc.gov
State-sponsored	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Federal agency roles	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Chief Information Officers (CIOs)	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov
Commerce	John F. Sargent, Jr.	7-9147	jsargent@crs.loc.gov
Defense (DOD)	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Executive Office of the President (EOP)	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Homeland Security (DHS)	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Intelligence Community (IC)	John Rollins	7-5529	jrollins@crs.loc.gov

Legislative Issues	Name/Title	Phone	Email
Justice (DOJ)	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
National Security Agency (NSA)	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Science agencies (NIST, NSF, OSTP)	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Treasury and financial agencies	Rena S. Miller	7-0826	rsmiller@crs.loc.gov
Federal Information Security Management Act (FISMA)	John D. Moteff	7-1435	jmoteff@crs.loc.gov
Federal Internet monitoring	Richard M. Thompson II	7-8449	rthompson@crs.loc.gov
Hacktivism	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
Information sharing	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Antitrust laws	Kathleen Ann Ruane	7-9135	kruane@crs.loc.gov
Civil liability	Edward C. Liu	7-9166	eliu@crs.loc.gov
Classified information	John Rollins	7-5529	jrollins@crs.loc.gov
Freedom of Information Act (FOIA)	Gina Stevens	7-2581	gstevens@crs.loc.gov
Privacy and civil liberties	Gina Stevens	7-2581	gstevens@crs.loc.gov
International cooperation			
Defense and diplomatic	Catherine A. Theohary	7-0844	ctheohary@crs.loc.gov
Law enforcement	Kristin M. Finklea	7-6259	kfinklea@crs.loc.gov
National strategy and policy	Eric A. Fischer	7-7071	efischer@crs.loc.gov
National security	John Rollins	7-5529	jrollins@crs.loc.gov
Public/private partnerships	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Supply chain	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Technological issues	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Botnets	Eric A. Fischer	7-7071	efischer@crs.loc.gov
Cloud computing	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov
Mobile devices	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov
Research and development (R&D)	Patricia Maloney Figliola	7-2508	pfigliola@crs.loc.gov