

Congressional Research Service

Informing the legislative debate since 1914

Cybersecurity: Authoritative Reports and Resources, by Topic

Rita Tehan
Information Research Specialist

December 4, 2013

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

CRS REPORT
Prepared for Members and Committees of Congress

c11173008

Summary

Cybersecurity vulnerabilities challenge governments, businesses, and individuals worldwide. Attacks have been initiated by individuals, as well as countries. Targets have included government networks, military defenses, companies, or political organizations, depending upon whether the attacker was seeking military intelligence, conducting diplomatic or industrial espionage, or intimidating political activists. In addition, national borders mean little or nothing to cyberattackers, and attributing an attack to a specific location can be difficult, which also makes a response problematic.

Congress has been actively involved in cybersecurity issues, holding hearings every year since 2001. There is no shortage of data on this topic: government agencies, academic institutions, think tanks, security consultants, and trade associations have issued hundreds of reports, studies, analyses, and statistics.

This report provides links to selected authoritative resources related to cybersecurity issues. It includes information on

- "CRS Reports by Topic"
  - Government Accountability Office (GAO) reports
  - White House/Office of Management and Budget reports
  - Military/DOD
  - Cloud Computing
  - Critical Infrastructure
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - Cybercrime/Cyberwar
  - International
  - Education/Training/Workforce
  - Research and Development (R&D)
- "Related Resources: Other Websites"

The report will be updated as needed.

c11173008

Contents

Introduction 1
CRS Reports by Topic 1
CRS Reports and Other CRS Products Overview: Cybersecurity Policy Framework 1
CRS Reports: Critical Infrastructure 32
CRS Reports and Other CRS Products: Cybercrime and National Security 41
Related Resources: Other Websites 67

Tables

Table 1. Selected Reports: Cybersecurity Overview 3
Table 2. Selected Government Reports: Government Accountability Office (GAO) 7
Table 3. Selected Government Reports: White House/Office of Management and Budget 14
Table 4. Selected Government Reports: Department of Defense (DOD) 17
Table 5. Selected Government Reports: National Strategy for Trusted Identities in Cyberspace (NSTIC) 22
Table 6. Selected Government Reports: Other Federal Agencies 23
Table 7. Selected Reports: Cloud Computing 29
Table 8. Selected Reports: Critical Infrastructure 33
Table 9. Selected Reports: Cybercrime/Cyberwar 42
Table 10. Selected Reports: International Efforts 49
Table 11. Selected Reports: Education/Training/Workforce 59
Table 12. Selected Reports: Research & Development (R&D) 64
Table 13. Related Resources: Congressional/Government 67
Table 14. Related Resources: International Organizations 69
Table 15. Related Resources: News 70
Table 16. Related Resources: Other Associations and Institutions 71

Contacts

Author Contact Information 72
Key Policy Staff 72

c11173008

Introduction

Cybersecurity is a sprawling topic that includes national, international, government, and private industry dimensions. In the 113th Congress, 5 bills have been introduced in the Senate and 7 in the House.[1] More than 40 bills and resolutions with provisions related to cybersecurity were introduced in the first session of the 112th Congress, including several proposing revisions to current laws. In the 111th Congress, the total was more than 60. Several of those bills received committee or floor action, but none became law. In fact, no comprehensive cybersecurity legislation has been enacted since 2002.

For Congressional Research Service (CRS) analysis, please see the collection of CRS reports found on the Issues in Focus: Cybersecurity site.

CRS Reports by Topic

This section gives references to analytical reports on cybersecurity from CRS, other governmental agencies, and trade organizations. The reports are grouped under the following cybersecurity topics: policy framework overview, critical infrastructure, and cybercrime and national security.

For each topic, CRS reports are listed first and then followed by tables with reports from other organizations. The overview reports provide an analysis of a broad range of cybersecurity issues (**Table 1** to **Table 7**). The critical infrastructure reports (**Table 8**) analyze cybersecurity issues related to telecom infrastructure, the electricity grid, and industrial control systems. The cybercrime and national security reports (**Table 9**) analyze a wide range of cybersecurity issues, including identify theft and government policies for dealing with cyberwar scenarios. In addition, tables with selected reports on international efforts to address cybersecurity problems, training for cybersecurity professionals, and research and development efforts in other areas are also provided (**Table 10** to **Table 12**).

CRS Reports and Other CRS Products Overview: Cybersecurity Policy Framework

- 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.

[1] For information on congressional cybersecurity activity in the 113th and 112th Congresses, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan. This report provides links to cybersecurity hearings and legislation under consideration in the 113th Congress and those considered in the 112th Congress, as well as executive orders and presidential directives. For selected statistics and glossaries, see CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan.

c11173008

- CRS Report R42409, *Cybersecurity: Selected Legal Issues*, by Edward C. Liu et al.
- CRS Report R43015, *Cloud Computing: Constitutional and Statutory Privacy Protections*, by Richard M. Thompson II
- CRS Legal Sidebar, *House Intelligence Committee Marks Up Cybersecurity Bill CISPA*, Richard M. Thompson II
- CRS Legal Sidebar, *Can the President Deal with Cybersecurity Issues via Executive Order?*, Vivian S. Chu

c11173008

.

Table 1. Selected Reports: Cybersecurity Overview

Title	Source	Date	Pages	Notes
Defending an Open, Global, Secure, and Resilient Internet http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836	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 http://www.safegov.org/media/46155/measuring_what_matters_final.pdf	Safegov.org, in coordination with the National Academy of Public Administration	March 2013	39	Rather than periodically auditing whether an agency's systems meet the standards enumerated in 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.
Developing a Framework To Improve Critical Infrastructure Cybersecurity (*Federal Register* Notice; Request for Information) http://www.gpo.gov/fdsys/pkg/FR-2013-02-26/pdf/2013-04413.pdf	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 http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key	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 demonstrates organizations' reluctance to share information within their own entities, industries, and across economic sectors.
The National Cyber Security Framework Manual http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf	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.

.

Title	Source	Date	Pages	Notes
Cyber Security Task Force: Public-Private Information Sharing http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf	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 http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf	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.
Mission Critical: A Public-Private Strategy for Effective Cybersecurity http://businessroundtable.org/uploads/studies-reports/downloads/2011_10_Mission_Critical_A_Public-Private_Strategy_for_Effective_Cybersecurity_4_20_12.pdf	Business Roundtable	October 11, 2011	28	According to the report, "[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.
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG) http://www.sans.org/critical-security-controls/	SANS	October 3, 2011	77	The 20 critical security control measures are intended to focus agencies and large enterprises' limited resources by plugging the most common attack vectors.
World Cybersecurity Technology Research Summit (Belfast 2011) http://www.csit.qub.ac.uk/InnovationatCSIT/Reports/Filetoupload,295594,en.pdf	Centre for Secure Information Technologies (CSIT)	September 12, 2011	14	The Belfast 2011 event attracted international cyber security experts from leading research institutes, government bodies, and industry who gathered to discuss current cyber security threats, predict future threats and the necessary mitigation techniques, and to develop a collective strategy for next research.

.

Title	Source	Date	Pages	Notes
A Review of Frequently Used Cyber Analogies http://www.nsci-va.org/WhitePapers/2011-07-22-Cyber-Analogies-Whitepaper-K-McKee.pdf	National Security Cyberspace Institute	July 22, 2011	7	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 http://www.cnas.org/node/6405	Center for a New American Security	June 1, 2011	296	To help U.S. policy makers address the growing danger of cyber insecurity, this two-volume report features chapters on cyber security 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 http://www.enisa.europa.eu/act/res/other-areas/inter-x/report/interx-report	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.
Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf	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 and makes a series of recommendations that build upon the conclusions of President Obama's *Cyberspace Policy Review*.
Cybersecurity Two Years Later http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf	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."

.

Title	Source	Date	Pages	Notes
Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop http://www.nap.edu/catalog.php?record_id=12998	National Research Council	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 recent reports from the NRC's Computer Science and Telecommunications Board on security and privacy.
National Security Threats in Cyberspace http://nationalstrategy.com/Portals/0/documents/National%20Security%20Threats%20in%20Cyberspace.pdf	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 CRS from the reports.

.

Table 2. Selected Government Reports: Government Accountability Office (GAO)

Title	Date	Pages	Notes
GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced http://www.gao.gov/products/GAO-14-15	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.
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts http://gao.gov/products/GAO-13-742	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 http://www.gao.gov/products/GAO-13-652T	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 http://www.gao.gov/products/GAO-13-275?source=ra	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 http://www.gao.gov/products/GAO-13-471	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), 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.

.

Title	Date	Pages	Notes
Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges http://www.gao.gov/products/GAO-13-462T	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."
2013 High Risk List http://www.gao.gov/highrisk#t=0	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 http://www.gao.gov/products/GAO-13-187	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 http://www.gao.gov/products/GAO-13-155	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 http://www.gao.gov/products/GAO-12-926T	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 http://www.gao.gov/products/GAO-12-756	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.

Title	Date	Pages	Notes
DOD Actions Needed to Strengthen Management and Oversight http://www.gao.gov/products/GAO-12-479?source=ra	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.
Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage http://www.gao.gov/products/GAO-12-876T	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 http://www.gao.gov/products/GAO-12-507T	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 http://www.gao.gov/products/GAO-12-92	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 http://www.gao.gov/products/GAO-12-8	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 http://www.gao.gov/products/GAO-11-634	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 http://www.gao.gov/products/GAO-12-130T	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.

Title	Date	Pages	Notes
Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements http://www.gao.gov/products/GAO-12-137	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.
Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management http://www.gao.gov/products/GAO-11-634	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 http://www.gao.gov/products/GAO-11-695R	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 http://www.gao.gov/products/GAO-11-463T	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 http://www.gao.gov/products/GAO-11-75	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 http://www.gao.gov/products/GAO-11-149	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.

Title	Date	Pages	Notes
Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems http://www.gao.gov/products/GAO-11-463T	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.
Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed http://www.gao.gov/products/GAO-11-117	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 http://www.gao.gov/products/GAO-11-43	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 http://www.gao.gov/products/GAO-11-24	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 http://www.gao.gov/products/GAO-10-772	September 23, 2010	46	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 http://www.gao.gov/products/GAO-10-916	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.

Title	Date	Pages	Notes
United States Faces Challenges in Addressing Global Cybersecurity and Governance http://www.gao.gov/products/GAO-10-606	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.
Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed http://www.gao.gov/products/GAO-10-628	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 http://www.gao.gov/products/GAO-10-513	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 http://www.gao.gov/products/GAO-10-834t	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 http://www.gao.gov/products/GAO-10-536t	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.

Title	Date	Pages	Notes
Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats http://www.gao.gov/products/GAO-11-463T	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.
Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies http://www.gao.gov/products/GAO-10-237	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 http://www.gao.gov/products/GAO-10-338	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 http://www.gao.gov/products/GAO-10-230t	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 http://www.gao.gov/products/GAO-03-760	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.

Source: Highlights compiled by CRS from the GAO reports.

.

Table 3. Selected Government Reports: White House/Office of Management and Budget

Title	Date	Pages	Notes
Immediate Opportunities for Strengthening the Nation's Cybersecurity http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf	November 2013	31	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 http://goals.performance.gov/node/39069	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 http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework	August 6, 2013	N/A	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.
Improving Cybersecurity http://technology.performance.gov/initiative/ensure-cybersecurity/home	March 2013	N/A	The Administration updated all 14 cross-agency priority goals on the Performance.gov portal, giving all new targets for agencies to hit over the next two years. OMB also is using the opportunity to better connect agency performance improvement officers to the TIC and Homeland Security.
FY 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002 http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf	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.

Title	Date	Pages	Notes
Administration Strategy for Mitigating the Theft of U.S. Trade Secrets http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf	February 20, 2013	141	"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 http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf	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 http://www.whitehouse.gov/blog/2012/08/01/collaborative-and-cross-cutting-approaches-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 http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf	December 6, 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.
Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-	October 7, 2011	N/A	President Obama signed an executive order outlining data security measures and rules for government agencies to follow to prevent further data leaks by insiders. The order included the creation of a senior steering committee that will oversee the safeguarding and sharing of information.
FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf	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.
International Strategy for Cyberspace http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf	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.

Title	Date	Pages	Notes
Cybersecurity Legislative Proposal (Fact Sheet) http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal	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.
Federal Cloud Computing Strategy http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf	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 http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf	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 http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf	July 6, 2010	39	This memorandum outlines and clarifies the respective responsibilities and activities of 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 http://www.dhs.gov/xlibrary/assets/ns_tic.pdf	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 creating an online environment, or an Identity Ecosystem, where individuals and organizations can complete online transactions with confidence, trusting the identities of each other and of the infrastructure where transaction occur.
Comprehensive National Cybersecurity Initiative (CNCI) http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative	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.
Cyberspace Policy Review: Assuring a Trusted and Resilient Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf	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 toward a reliable, resilient, trustworthy digital infrastructure for the future.

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

c11173008

.

Table 4. Selected Government Reports: Department of Defense (DOD)

Title	Source	Date	Pages	Notes
Offensive Cyber Capabilities at the Operational Level—The Way Ahead https://csis.org/publication/offensive-cyber-capabilities-operational-level	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 http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1170.pdf	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, 20123	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. Although these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists.
Military and Security Developments Involving the People's Republic of China 2013 (Annual Report to Congress) http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf	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.

.

Title	Source	Date	Pages	Notes
Resilient Military Systems and the Advanced Cyber Threat http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf	Department of Defense 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.
FY 2012 Annual Report http://www.dote.osd.mil/pub/reports/FY2012/pdf/other/2012DOTEAnnualReport.pdf	Department of Defense	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) http://www.gpo.gov/fdsys/pkg/FR-2012-08-24/pdf/2012-20881.pdf	Department of Defense (DOD), General Services Administration (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)."
DOD Actions Needed to Strengthen Management and Oversight http://www.gao.gov/products/GAO-12-479?source=ra	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 http://www.defense.gov/news/DoDCloudComputingStrategy.pdf	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 Activities http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf	*Federal Register*	May 11, 2012		DOD interim final rule to establish a voluntary cyber security 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 http://www.fas.org/sgp/othergov/dod/5200_01v1.pdf	DOD	February 16, 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 http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA561779&Location=U2&doc=GetTRDoc.pdf	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 http://www.gao.gov/products/GAO-11-695R	Government Accountability Office (GAO)	July 29, 2011	33	This letter discusses DOD's cyber and information assurance budget for fiscal year 2012 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.

.

Title	Source	Date	Pages	Notes
Legal Reviews of Weapons and Cyber Capabilities http://www.fas.org/irp/doddir/usaf/afi51-402.pdf	Secretary of the Air Force	July 27, 2011	7	States 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.
Department of Defense Strategy for Operating in Cyberspace http://www.defense.gov/news/d20110714cyber.pdf	DOD	July 14, 2011	19	This is an unclassified summary of DOD's cyber-security strategy.
Cyber Operations Personnel Report (DOD) http://www.hsdl.org/?view&did=488076	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) http://info.publicintelligence.net/DARPA-ADAMS.pdf	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 http://www.nap.edu/catalog.php?record_id=12979	National Research Council, Committee for Advancing Software-Intensive Systems Producibility	October 20, 2010	161	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.

.

Title	Source	Date	Pages	Notes
Defending a New Domain http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain	U.S. Deputy Secretary of Defense, William J. Lynn (Foreign Affairs)	September 2010	N/A	In 2008, the U.S. Department of Defense 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) http://www.usip.org/quadrennial-defense-review-independent-panel-/view-the-report	Quadrennial Defense Review	July 30, 2010	159	From the report: "The expanding cyber mission also needs to be examined. The Department of Defense should be prepared to assist civil authorities in defending cyberspace – beyond the Department's current role."
Cyberspace Operations: Air Force Doctrine Document 3-12 http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf	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.
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.

.

Table 5. Selected Government Reports: National Strategy for Trusted Identities in Cyberspace (NSTIC)

Title	Source	Date	Pages	Notes
NIST Awards Grants to Improve Online Security and Privacy http://www.nist.gov/itl/nstic-091713.cfm	NIST	September 17, 2013	N/A	NIST announced more than $7 million in grants to support the National Strategy for Trusted Identities in Cyberspace (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 http://www.nist.gov/itl/nstic-092012.cfm	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 for the National Strategy for Trusted Identities in Cyberspace http://www.nist.gov/nstic/2012-nstic-governance-recs.pdf	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.
Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace http://www.nist.gov/nstic/nstic-frn-noi.pdf	Department of Commerce	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	52	Press release on a proposal to administer the processes for policy and standards adoption for the Identity Ecosystem Framework in accordance with the NSTIC.
National Strategy for Trusted Identities in Cyberspace	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 Cyberspace: Creating Options for Enhanced Online Security and Privacy (Draft)	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 6. Selected Government Reports: Other Federal Agencies

Title	Source	Date	Pages	Notes
Evaluation of DHS' Information Security Program for Fiscal Year 2013 http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-09_Nov13.pdf	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 http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf	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.
Cybersecurity Framework http://www.nist.gov/itl/cyberframework.cfm	NIST	October 22, 2013	47	NIST seeks comments on the preliminary version of the Cybersecurity Framework ("preliminary Framework"). Under Executive Order 13636, the Secretary of Commerce is tasked to direct the director of NIST to work with stakeholders to develop a framework to reduce cyber risks to critical infrastructure.
DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Center http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf	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.

Title	Source	Date	Pages	Notes
Federal Energy Regulatory Commission's Unclassified Cyber Security Program – 2013 http://energy.gov/sites/prod/files/2013/10/f4/OAS-M-14-01.pdf	Department of Energy Office of Inspector General	October 2013	13	To help protect against continuing cyber security threats, the commission estimated that it would spend approximately $5.8 million during FY2013 to secure its information technology assets, a 9% increase compared with FY2012 As directed by FISMA, the Office of Inspector General conducted an independent evaluation of the Commission's Unclassified Cyber Security program to determine whether it adequately protected data and information systems. This report presents the results of our evaluation for FY2013.
Discussion Draft of the Preliminary Cybersecurity Framework http://nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf	NIST	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; and (5) foster communications among internal and external stakeholders.
Special Cybersecurity Workforce Project (Memo for Heads of Executive Departments and Agencies) http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=5716	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.
Guide to Malware Incident Prevention and Handling for Desktops and Laptops http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf	NIST	July 1, 2013	47	Provides recommendations for improving an organization's malware incident prevention measures. Also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones.
DRAFT Outline—Preliminary Framework to Reduce Cyber Risks to Critical Infrastructure http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf	NIST	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.

Title	Source	Date	Pages	Notes
Computer Security Incident Coordination (CSIC): Providing Timely Cyber Incident Response http://www.gpo.gov/fdsys/pkg/FR-2013-06-28/pdf/2013-15542.pdf	NIST	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 http://www.gpo.gov/fdsys/pkg/FR-2013-06-21/pdf/2013-14897.pdf	NIST	June 21, 2013	3	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. 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 http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_061813.pdf	NIST	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.
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices http://www.gpo.gov/fdsys/pkg/FR-2013-06-14/pdf/2013-14167.pdf	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 in order to maintain information confidentiality, integrity, and availability.
DHS Can Take Actions to Address Its Additional Cybersecurity Responsibilities http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-95_Jun13.pdf	Department of Homeland Security	June 5, 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.

.

Title	Source	Date	Pages	Notes
Mobile Security Reference Architecture https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf	Federal CIO Council and the Department of Homeland Security (DHS)	May 23, 2013	104	Gives agencies guidance in the secure implementation of mobile solutions through their enterprise architectures. The document provides in-depth reference architecture for mobile computing.
Initial Analysis of Cybersecurity Framework RFI Responses http://csrc.nist.gov/cyberframework/rfi_initial_responses.html	NIST	May 15, 2013	34	This document represents NIST's initial analysis of the Request for Information (RFI) responses. Its purpose is to describe the methodology that NIST used to perform the initial analysis of the submitted responses, and to identify and describe the Cybersecurity Framework themes that emerged as a part of the initial analysis.
Proposed Establishment of a Federally Funded Research and Development Center-First Notice http://www.gpo.gov/fdsys/pkg/FR-2013-04-22/pdf/2013-09376.pdf	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.
Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A) http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf	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).
Cyber Student Initiative http://www.dhs.gov/sites/default/files/publications/SHP_Cyber_Student_Initiative_Bulletin.pdf	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.

.

Title	Source	Date	Pages	Notes
Security and Privacy Controls for Federal Information Systems (SP 800-53) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf	NIST	April 2013	3	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.
Guide to Attribute Based Access Control Definition and Consideration (SP 800-162)	NIST	April 2013	54	Improving information sharing while maintaining control over access to that information is a primary goal of guidance coming from the NIST.
National Level Exercise 2012: Quick Look Report http://www.fema.gov/library/viewRecord.do?id=7240	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.
Measuring What Matters: Reducing Risks by Rethinking How We Evaluate Cybersecurity http://www.safegov.org/media/46155/measuring_what_matters_final.pdf	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.
Developing a Framework To Improve Critical Infrastructure Cybersecurity http://www.gpo.gov/fdsys/pkg/FR-2013-02-26/pdf/2013-04413.pdf	National Institute of Standards and Technology (NIST)	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.

.

Title	Source	Date	Pages	Notes
Follow-up Audit of the Department's Cyber Security Incident Management Program https://www.hsdl.org/?view&did=728459	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 http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709	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).
Information Sharing Environment: Annual Report to Congress 2012 http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf	Information Sharing Environment (ISE)	June 30, 2012	188	"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."
Cybersecurity: CF Disclosure Guidance: Topic No. 2 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm	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 7. Selected Reports: Cloud Computing

Title	Source	Date	Pages	Notes
Delivering on the Promise of Big Data and the Cloud http://www.boozallen.com/media/file/BigDataInTheCloud.pdf	Booz, Allen, Hamilton	January 9, 2013	7	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 http://judiciary.house.gov/hearings/Hearings%202012/hear_07252012_2.html	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 http://www.gao.gov/products/GAO-12-756	GAO	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 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 http://www.defense.gov/news/DoDCloudComputingStrategy.pdf	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.
A Global Reality: Governmental Access to Data in the Cloud - A Comparative Analysis of Ten International Jurisdictions http://www.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf	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.

Title	Source	Date	Pages	Notes
Policy Challenges of Cross-Border Cloud Computing http://www.usitc.gov/journals/Policy_Challenges_of_Cross-border_Cloud_Computing_rev.pdf	U.S. International Trade Commission	May 1, 2012	38	Examine 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.
Cloud Computing Synopsis and Recommendations http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf	NIST	May 2012	81	The National Institute of Standards and Technology has unveiled a guide that 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 http://portal.bsa.org/cloudscorecard2012/	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 http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf	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) http://www.gsa.gov/portal/category/102371	Federal CIO Council	January 4, 2012	N/A	The Federal Risk and Authorization Management Program or 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) http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf	White House/Office of Management and Budget (OMB)	December 8, 2011	7	The Federal Risk and Authorization Management Program (FedRAMP) will now be required for all agencies purchasing storage, applications and other remote services from vendors. The Obama Administration has championed 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 http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf	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.

.

Title	Source	Date	Pages	Notes
U.S. Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf	NIST	December 1, 2011	85	Volume II is designed to be a technical reference for those actively working on strategic and tactical cloud computing initiatives, including, but not limited to, U.S. government cloud adopters. Volume II integrates and summarizes the work completed to date, and explains how these findings support the roadmap introduced in Volume I.
Information Security: Additional Guidance Needed to Address Cloud Computing Concerns http://www.gao.gov/products/GAO-12-130T	GAO	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. NIST has issued multiple publications which address such guidance; however, one publication remains in draft, and is not to be finalized until the first quarter of fiscal year 2012.
Cloud Computing Reference Architecture http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505	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 http://www.siia.net/index.php?option=com_docman&task=doc_download&gid=3040&Itemid=318	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 http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf	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.

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 R42351, *Internet Governance and the Domain Name System: Issues for Congress*, by Lennard G. Kruger

c11173008

Table 8. Selected Reports: Critical Infrastructure

Title	Source	Date	Pages	Notes
The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities http://www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf	Brookings Institution/ Center for 21st Century Security and Intelligence	July 2013	50	The study argues that the level of cyber security 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 http://op.bna.com/bar.nsf/id/jtin-98errp/$File/ffieccyber.pdf	Federal Financial Institutions Examination Council (FFIEC)	June 6, 2013	2	FFIEC announced the formation of 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 http://markey.house.gov/sites/markey.house.gov/files/documents/Markey%20Grid%20Report_05.21.13.pdf	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.
Initial Analysis of Cybersecurity Framework RFI Responses http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf	National Institute of Standards and Technology	May 20, 2013	33	Comments on the challenges of protecting the nation's critical infrastructure have identified a handful of top-of-mind 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 http://www.gpo.gov/fdsys/pkg/FR-2013-05-13/pdf/2013-11239.pdf	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.

.

Title	Source	Date	Pages	Notes
Version 5 Critical Infrastructure Protection Reliability Standards (Notice of Proposed Rulemaking) http://www.gpo.gov/fdsys/pkg/FR-2013-04-24/pdf/2013-09643.pdf	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 cyber security of the bulk electric system, represent an improvement over the current Commission-approved CIP Reliability Standards as they adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards.
Incentives To Adopt Improved Cybersecurity Practices http://www.ntia.doc.gov/federal-register-notice/2013/notice-inquiry-incentives-adopt-improved-cybersecurity-practices-html	National Institute of Standards and Technology and the National Telecommunications and Information Administration	March 28, 2013	N/A	The Commerce Department is preparing a report on 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.
SCADA and Process Control Security Survey https://www.sans.org/reading_room/analysts_program/sans_survey_scada_2013.pdf	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.
Follow-up Audit of the Department's Cyber Security Incident Management Program https://www.hsdl.org/?view&did=728459	U.S. Department of Energy Inspector General's Office	December 1, 2012	25	In 2008, it was 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 the prior report, identified were several issues that limited the efficiency and effectiveness of the department's cyber security 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.

Title	Source	Date	Pages	Notes
Terrorism and the Electric Power Delivery System http://www.nap.edu/catalog.php?record_id=12050	National Academies of Science	November 2012	146	Focuses on measures that could make the power delivery system less vulnerable to attacks, restore power faster after an attack, and make critical services less vulnerable while the delivery of conventional electric power has been disrupted.
New FERC Office to Focus on Cyber Security http://www.ferc.gov/media/news-releases/2012/2012-3/09-20-12.asp	U.S. Department of Energy	September 20, 2012	N/A	The Federal Energy Regulatory Commission 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, as well as other agencies and private companies, better identify potential dangers and solutions.
Canvassing the Targeting of Energy Infrastructure: The Energy Infrastructure Attack Database http://www.ensec.org/index.php?option=com_content&view=article&id=379:canvassing-the-targeting-of-energy-infrastructure-the-energy-infrastructure-attack-database&catid=128:issue-content&Itemid=402	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 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 http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/TheCIPReport_August2012_SmartGrid.pdf	Center for Infrastructure Protection and Homeland Security, George Mason School of Law	August 1, 2012	26	Highlights the significance of and the challenges with securing the smart grid.
Cybersecurity: Challenges in Securing the Electricity Grid http://www.gao.gov/products/GAO-12-926T	GAO	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.
ICS-CERT Incident Response Summary Report (2009-2011) http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf	U.S. Industrial Control System Cyber Emergency Response Team (ICS-CERT)	June 28, 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.

Title	Source	Date	Pages	Notes
Energy Department Develops Tool with Industry to Help Utilities Strengthen Their Cybersecurity Capabilities http://energy.gov/articles/energy-department-develops-tool-industry-help-utilities-strengthen-their-cybersecurity	U.S. Department of Energy	June 28, 2012	N/A	The Cybersecurity Self-Evaluation Tool utilizes 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.
Electricity Subsector Cybersecurity Risk Management Process http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012	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.
Cybersecurity for Energy Delivery Systems Program http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity	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.
ICT Applications for the Smart Grid: Opportunities and Policy Implications http://www.oecd-ilibrary.org/content/workingpaper/5k9h2q8v9bln-en	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 http://energy.gov/ig/downloads/departments-management-smart-grid-investment-grant-program-oas-ra-12-04	Department of Energy (DOE) Inspector General	January 1, 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.
Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use http://www.gao.gov/products/GAO-12-92	Government Accountability Office (GAO)	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 available guidance could help both federal and private-sector decision makers better coordinate their efforts to protect critical cyber-reliant assets.

Title	Source	Date	Pages	Notes
The Future of the Electric Grid http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml	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 ftp://ftp.fcc.gov/pub/Daily_Releases/Daily_Business/2011/db0610/DOC-307454A1.txt	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 http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=1067	U.S. Army War College	May 9, 2011	324	Part 1 deals with strategic and policy issues related to cybersecurity 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 http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf	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
Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems http://www.gao.gov/products/GAO-11-463T	Government Accountability Office (GAO)	March 16, 2011	16	According to GAO, executive branch agencies have also 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.

Title	Source	Date	Pages	Notes
Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security http://www.wired.com/images_blogs/threatlevel/2011/02/DoE-IG-Report-on-Grid-Security.pdf	North American Electric Reliability Corp. (NERC)	January 26, 2011	30	NERC developed Critical Infrastructure Protection (CIP) cyber security reliability standards which were approved by the FERC in January 2008. Although the Commission had taken steps to ensure CIP cyber security 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 http://www.gao.gov/products/GAO-11-117	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 should assess whether any cybersecurity challenges identified in this report should be addressed in the guidelines.
Partnership for Cybersecurity Innovation http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation	White House (Office of Science & Technology Policy)	December 6, 2010	4	The Obama Administration released a Memorandum of Understanding signed by the National Institute of Standards and Technology (NIST) 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 the nation's critical infrastructures.
WIB Security Standard Released http://www.isssource.com/wib/	International Instrument Users Association (WIB)	November 10, 2010		The Netherlands-based International Instrument Users Association (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 cyber security best practices for suppliers of industrial automation and control systems.

Title	Source	Date	Pages	Notes
Information Security Management System for Microsoft Cloud Infrastructure http://cdn.globalfoundationservices.com/documents/InformationSecurityMangSysforMSCloudInfrastructure.pdf	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 http://www.nist.gov/public_affairs/releases/nist-finalizes-initial-set-of-smart-grid-cyber-security-guidelines.cfm	National Institute of Standards and Technology (NIST)	September 2, 2010	N/A	NIST released a three-volume set of recommendations on all things 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 http://www.gao.gov/products/GAO-10-628	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 http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx	Pew Research Center's Internet & American Life Project	June 11, 2010	26	Technology experts and stakeholders say they 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) http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf	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.
NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses http://www.fas.org/sgp/eprint/nstb.pdf	Department of Energy, Idaho National Laboratory	May 1, 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 http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-305618A1.doc	Federal Communications Commission (FCC)	April 21, 2010	N/A	The Federal Communications Commission launched an inquiry on 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.

.

Title	Source	Date	Pages	Notes
Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 http://www.cloudsecurityalliance.org/csaguide.pdf	Cloud Security Alliance	December 2009	76	"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 http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf	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 Legal Sidebar, Legal Barriers to an Expanded Role of the Military in Defending Against Domestic Cyberattacks, Andrew Nolan

  CRS Legal Sidebar, Obstacles to Private Sector Cyber Threat Information Sharing, Edward C. Liu

c11173008

.

Table 9. Selected Reports: Cybercrime/Cyberwar

Title	Source	Date	Pages	Notes
Cyber-Warfare: Is the risk of cyber-warfare overrated? http://www.economist.com/debate/days/view/997	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."
ThreatWatch http://www.nextgov.com/cybersecurity/threatwatch/	NextGov	August 2013	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, because many compromises are never reported or even discovered. The information is based on accounts published by outside news organizations and researchers.
The Economic Impact of Cybercrime and Cyber Espionage http://csis.org/publication/economic-impact-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.
Electric Grid Vulnerability: Industry Responses Reveal Security Gaps http://markey.house.gov/sites/markey.house.gov/files/documents/Markey%20Grid%20Report_05.21.13.pdf	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.
Towards Trustworthy Social Media and Crowdsourcing http://www.scribd.com/doc/138508756/Towards-Trustworthy-Social-Media-and-Crowdsourcing#download	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 http://americanmanufacturing.org/files/RemakingAmericanSecurityMay2013.pdf	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.

.

Title	Source	Date	Pages	Notes
Role of Counterterrorism Law in Shaping 'ad Bellum' Norms for Cyber Warfare https://www.hsdl.org/?view&did=734375	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 http://ccdcoe.org/249.html	Cambridge University Press/ NATO Cooperative Cyber Defence Center of Excellence	March 5, 2013	282	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 http://intelreport.mandiant.com/ Mandiant_APT1_Report.pdf	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 http://intelreport.mandiant.com/	Mandiant	February 19, 2013	N/A	Video of APT1 attacker sessions and intrusion activities (5-minute video).
Crisis and Escalation in Cyberspace http://www.rand.org/pubs/monographs/MG1215.html	RAND Corp.	December 2012	200	The genesis for this work was the broader issue of 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) http://www.foreignaffairs.com/cyberattacks-by-initiator-and-victim	Foreign Affairs	November 21, 2012	N/A	A chart showing cyberattacks by initiator and victim, 2001-2011.
Emerging Cyber Threats Report 2013 http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf	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 http://prod.sandia.gov/techlib/access-control.cgi/2012/1210177.pdf	Sandia National Labs	November 1, 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 http://www.isn.ethz.ch/isn/Editorial-Plan/Dossiers/Detail/?lng=en&id=154059&contextid782=154059	International Relations and Security Network (ISN)	October 22, 2012	N/A	Looks at the Militarisation of Cyber Security 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 http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf	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.
ZeroAccess: We're Gonna Need a Bigger Planet http://www.f-secure.com/weblog/archives/00002428.html	F-Secure and Google Maps	October 15, 2012	N/A	The idea of a network of malware-infected zombie computers rigged to do the bidding of criminals conjures up a frightening image on its own. A new visualization of the so-called ZeroAcess botnet shows how widespread such schemes can become.
Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE http://intelligence.house.gov/press-release/investigative-report-us-national-security-issues-posed-chinese-telecommunications	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.

Title	Source	Date	Pages	Notes
Federal Support for and Involvement in State and Local Fusion Centers http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04	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.
HoneyMap—Visualizing Worldwide Attacks in Real-Time http://www.honeynet.org/node/960	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.
Manual on International Law Applicable to Cyber Warfare ("The Tallinn Manual") http://www.ccdcoe.org/249.html	NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia	August 2012	N/A	The Tallinn Manual is a nonbinding yet authoritative restatement of the law of armed conflict as it relates to cyberwar. It offers guidance to attackers, defenders, and legal experts on how cyberattacks can be classified as actions covered under the law, such as armed attacks.
Does Cybercrime Really Cost $1 Trillion? http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion	ProPublica	August 1, 2012	N/A	In a news release from computer security firm McAfee to announce its 2009 report, "Unsecured Economies: Protecting Vital Information," the company 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.
Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3848/3270	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 cyber security challenges, including the as-yet unrealized possibility of cyber war.
Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage http://www.gao.gov/products/GAO-12-876T	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.

Title	Source	Date	Pages	Notes
Measuring the Cost of Cybercrime http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf	11th Annual Workshop on the Economics of Information Security	June 25, 2012	N/A	"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."
Nodes and Codes: The Reality of Cyber Warfare http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA567190&Location=U2&doc=GetTRDoc.pdf	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.
The Impact of Cybercrime on Businesses http://www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf	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 http://www.oecd-ilibrary.org/science-and-technology/proactive-policy-measures-by-internet-service-providers-against-botnets_5k98tq42t18w-en	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 http://www.nass.org/index.php?option=com_docman&task=doc_download&gid=1257	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.
A Cyberworm that Knows No Boundaries http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf	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 http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf	DOD	November 15, 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."

.

Title	Source	Date	Pages	Notes
W32.Duqu: The Precursor to the Next Stuxnet http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet	Symantec	October 24, 2011	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.
Cyber War Will Not Take Place http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939	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.
Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG) http://www.sans.org/critical-security-controls/	SANS	October 3, 2011	77	The 20 measures are intended to focus agencies' limited resources on plugging the most common attack vectors.
Revealed: Operation Shady RAT: an Investigation Of Targeted Intrusions Into 70+ Global Companies, Governments, and Non-Profit Organizations During the Last 5 Years http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf	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.
USCYBERCOM and Cyber Security: Is a Comprehensive Strategy Possible? http://handle.dtic.mil/100.2/ADA565051	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 http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-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."

.

Title	Source	Date	Pages	Notes
Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/	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.
The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis Bases on Spam Data http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.2211&rep=rep1&type=pdf	Organisation for Economic Co-operation and Development	November 12, 2010	68	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.
Stuxnet Analysis http://www.enisa.europa.eu/media/press-releases/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 http://www.nap.edu/catalog.php?record_id=12997#description	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.
Untangling Attribution: Moving to Accountability in Cyberspace [Testimony] http://i.cfr.org/content/publications/attachments/Knake%20-Testimony%20071510.pdf	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 http://www.nap.edu/catalog.php?record_id=12651&utm_medium=etmail&utm_source=National%20Academies%20Press&utm_campaign=NAP+mail+eblast+10.27.09+-+Cyberattack+Preorder+sp&utm_content=Downloader&utm_term=#description	National Research Council	January 1, 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 10. Selected Reports: International Efforts

Title	Source	Date	Pages	Notes
Confidence Building Measures and International Cybersecurity http://ict4peace.org/what-next-building-confidence-measures-for-the-cyberspace/	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.
Directive of the European Parliament and of the Council on Attacks Against Information Systems http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF	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).
FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol	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. This group will begin its practical activities within the next month.

.

Title	Source	Date	Pages	Notes
Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment http://www.gao.gov/products/GAO-13-652T	General 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 http://www.da.mod.uk/publications/library/technology/20130508-Cyber_report_final_U.pdf/view	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.
Military and Security Developments Involving the People's Republic of China 2013 (Annual Report to Congress) http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf	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.

Title	Source	Date	Pages	Notes
Defence White Paper 2013 http://www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf	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 http://americanmanufacturing.org/files/RemakingAmericanSecurityMay2013.pdf	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) https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security	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. The Cyber Security Information Sharing Partnership 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.
The Tallinn Manual on the International Law Applicable to Cyber Warfare http://ccdcoe.org/249.html	Cambridge University Press/ NATO Cooperative Cyber Defence Center of Excellence	March 5, 2013	282	The Tallinn Manual identifies the international law applicable to cyber warfare and sets out ninety-five '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
Administration Strategy for Mitigating the Theft of U.S. Trade Secrets http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf	White House	February 20, 2013	141	"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."
APT1: Exposing One of China's Cyber Espionage Units http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf	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 http://intelreport.mandiant.com/	Mandiant	February 19, 2013	N/A	Video of APT1 attacker sessions and intrusion activities (5-minute video).
Worldwide Threat Assessment of the U.S. Intelligence Community (Testimony) http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf	James Clapper, Director of National Intelligence	February 11, 2013	34	Clapper provided an assessment of global cybersecurity threats: U.S. critical infrastructure, eroding U.S. economic and national security, information control and Internet governance, and hactivists and criminals.

.

Title	Source	Date	Pages	Notes
An Open, Safe and Secure Cyberspace http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security	European Union	February 7, 2013	20	The strategy articulates the EU's vision of cyber-security in terms of five priorities: achieving cyber resilience; drastically reducing cybercrime; developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); developing the industrial and technological resources for cyber-security; establishing a coherent international cyberspace policy for the European Union and promoting core EU values.
Linking Cybersecurity Policy and Performance http://blogs.technet.com/b/trustworthycomputing/archive/2013/02/06/linking-cybersecurity-policy-and-performance-microsoft-releases-special-edition-security-intelligence-report.aspx	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. Examine 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.
The Chinese Defense Economy Takes Off: Sector-by-Sector Assessments and the Role of Military End-Users http://igcc.ucsd.edu/assets/001/504355.pdf	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.

Title	Source	Date	Pages	Notes
Defence and Cyber-Security, vol. 1 - Report, together with formal minutes, oral and written evidence http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf Defence and Cyber-Security, vol. 2 - Additional Written Evidence http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106vw.pdf	House of Commons Defence Committee (UK)	December 18, 2012	51 (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.
The Challenge of Cyber Power for Central African Countries: Risks and Opportunities http://handle.dtic.mil/100.2/ADA576285	Naval Postgraduate School	December 2012	209	"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 http://oecdinsights.org/2012/11/29/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 will take 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 http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf	Organization for Economic Co-operation and Development	November 16, 2012	57	This report analyses the latest generation of national cybersecurity strategies in ten OECD countries and identifies commonalities and differences.

.

Title	Source	Date	Pages	Notes
2012 Report to Congress of the U.S.-China Economic and Security Review Commission, One Hundred Twelfth Congress, Second Session, November 2012 https://www.hsdl.org/?view&did=725530	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 http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/1998792/upload_binary/1998792.pdf	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.
More Than Meets the Eye: Clandestine Funding, Cutting-Edge Technology and China's Cyber Research & Development Program http://www.osti.gov/bridge/servlets/purl/1055833/	Lawrence Livermore National Laboratory	October 23, 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 http://intelligence.house.gov/press-release/investigative-report-us-national-security-issues-posed-chinese-telecommunications	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.

.

Title	Source	Date	Pages	Notes
Manual on International Law Applicable to Cyber Warfare ("The Tallinn Manual") http://www.ccdcoe.org/249.html	NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia	August 2012	N/A	The Tallinn Manual is a nonbinding yet authoritative restatement of the law of armed conflict as it relates to cyberwar. It offers attackers, defenders, and legal experts guidance on how cyberattacks can be classified as actions covered under the law, such as armed attacks.
Bilateral Discussions on Cooperation in Cybersecurity http://www.cicir.ac.cn/chinese/newsView.aspx?nid=3878	China Institute of Contemporary International Relations and the Center for Strategic and International Studies (CSIS)	June 2012	N/A	(Scroll down for English). 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? http://www.ndc.nato.int/download/downloads.php?icode=334	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, e-mail, 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.
Cyber-security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness Around the World http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048	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.

Title	Source	Date	Pages	Notes
Cyber Power Index http://www.cyberhub.com/CyberPowerIndex	Booz Allen Hamilton and the Economist Intelligence Unit	January 15, 2012	N/A	The index of developing countries' ability to withstand cyberattacks and build strong digital economies, rates the countries on their legal and regulatory frameworks; economic and social issues; technology infrastructure; and industry. The index puts the United States in the No. 2 spot, and the UK in No. 1.
Foreign Spies Stealing US Economic Secrets in Cyberspace http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf	Office of the National Counterintelligence Executive	November 3, 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.
The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf	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 cyber security in 2015.
Cyber Dawn: Libya http://www.unveillance.com/wp-content/uploads/2011/05/Project_Cyber_Dawn_Public.pdf	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.
International Strategy for Cyberspace http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf	White House	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.
China's Cyber Power and America's National Security http://www.dtic.mil/dtic/tr/fulltext/u2/a552990.pdf	U.S. Army War College, Strategy Research Project	March 24, 2011	86	This report examines the growth of Chinese cyber power; their known and demonstrated capabilities for offensive, defensive and exploitive computer network operations; China's national security objectives; and the possible application of Chinese cyber power in support of those objectives.

.

Title	Source	Date	Pages	Notes
Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace http://vialardi.org/nastrazzuro/pdf/US-Russia.pdf	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) http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf	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.
ITU Toolkit for Cybercrime Legislation http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf	International Telecommunications Union	February 2010	N/A	This document aims to provide countries with sample legislative language and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules.

Note: Highlights compiled by CRS from the reports.

.

Table 11. Selected Reports: Education/Training/Workforce

Title	Source	Date	Pages	Notes
DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts http://gao.gov/products/GAO-13-742	GAO	September 17, 2013	47	More than one in five jobs at a key cybersecurity component within the Homeland Security Department are 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 http://www.nap.edu/catalog.php?record_id=18446	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 http://pellcenter.salvereginablogs.com/files/2013/08/JPME-Cyber-Leaders-Final.pdf	Pell Center	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. Although these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists.
Pay Under the General Schedule and Recruitment, Relocation, and Retention Incentives http://www.gpo.gov/fdsys/pkg/FR-2013-08-14/pdf/2013-19641.pdf	Office of Personnel Management (OPM)	August 14, 2013	6	OPM outlined changes to the way agencies evaluate and award recruitment, retention and relocation (3R) bonuses—changes that could affect how agencies hire and keep employees with essential technology skills. The new rules take effect September 13.

.

Title	Source	Date	Pages	Notes
U.S.A. Cyber Warrior Scholarship Program https://www.isc2cares.org/USA-Cyber-Warrior-Scholarship/default.aspx	(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 https://www.isc2.org/workforcestudy/default.aspx	(ISC)² and Frost & Sullivan	May 7, 2013	28	Federal cyber workers earn an average salary of $106,430, quite a bit 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.
NCCoE Celebrates National Cybersecurity Excellence Partnerships http://csrc.nist.gov/nccoe/The-Center/News/News.html	NIST National Cybersecurity Center of Excellence	April 15, 2013	N/A	Eleven private organizations agreed to partner with the National Institute of Standards and Technology to share cybersecurity staff and best practices to help better combat cyber threats.
2012 Information Technology Workforce Assessment for Cybersecurity https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf	U.S. Department of Homeland Security	April 3, 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.
National Initiative for Cybersecurity Careers and Studies (NICCS) http://niccs.us-cert.gov/	U.S. Department of Homeland Security	February 21, 2013	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.
Michigan Cyber Range http://www.merit.edu/cyberrange/	Partnership between the state of Michigan, Merit Network, federal and local governments, colleges and universities, and the private sector	November 12, 2012	N/A	Enables individuals and organizations to develop detection and reaction skills through simulations and exercises.

Title	Source	Date	Pages	Notes
CyberSkills Task Force Report https://www.hsdl.org/hslog/?q=node/7934	U.S. Department of Homeland Security	October 1, 2012	41	DHS's Task Force on CyberSkills proposes far-reaching improvements to enable DHS to recruit and retain the cybersecurity talent it needs.
Cyber Security Test Bed: Summary and Evaluation Results http://sites.duke.edu/ihss/files/2011/12/Cyber-Security-Test-Bed_Final-Report_Rowe.pdf	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.
Information Assurance Scholarship Program http://www.doncio.navy.mil/ContentView.aspx?id=535	U.S Navy	August 28, 2012	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, Defense officials said last week. The scholarships also are an attempt to effectively retain military and civilian cybersecurity and IT personnel.
Preparing the Pipeline: The U.S. Cyber Workforce for the Future http://handle.dtic.mil/100.2/ADA577318	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 http://www.pnl.gov/main/publications/external/technical_reports/PNNL-21639.pdf	Pacific Northwest National Laboratory	August 1, 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
National Centers of Academic Excellence (CAE) in Cyber Operations Program http://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml	National Security Agency (NSA)	May 29, 2012	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.
Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination http://www.gao.gov/products/GAO-12-8	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 NICE initiative 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 http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505	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.
2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey http://www.staysafeonline.org/sites/default/files/resource_documents/2011%20National%20K-12%20Study%20Final_0.pdf	National Cyber Security Alliance and Microsoft	May 13, 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. This year's 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 (DOD) http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf	Department of Defense	April 2011	84	This report is focused on FY09 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
Design of the DETER Security Testbed http://www.isi.edu/deter/news/news.php?story=20	University of Southern California (USC) Information Sciences Institute, University of California Berkeley (UCB), McAfee Research	January 13, 2011	N/A	The Department of Homeland Security (DHS) will invest $16 million over the next five years to expand a cybersecurity testbed at the University of Southern California (USC). The Deterlab testbed provides an isolated 400-node mini-Internet, in which researchers can investigate malware and other security threats without danger of infecting the real Internet. It also supports classroom exercises in computer security for nearly 400 students at 10 universities and colleges.
The Power of People: Building an Integrated National Security Professional System for the 21st Century http://www.pnsr.org/data/images/pnsr_the_power_of_people_report.pdf	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.

c11173008

Table 12. Selected Reports: Research & Development (R&D)

Title	Source	Date	Pages	Notes
Cyber Grand Challenge for automated network security-correcting systems http://www.darpa.mil/NewsEvents/Releases/2013/10/22.aspx	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.
Cybersecurity Exercise: Quantum Dawn 2 http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/	SIFMA	June 28, 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 http://www.gpo.gov/fdsys/pkg/FR-2013-06-21/pdf/2013-14897.pdf	National Institute of Standards and Technology	June 21, 2013	3	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. 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.
Open Trusted Technology Provider Standard (O-TTPS)™, Version 1.0: Mitigating Maliciously Tainted and Counterfeit Products https://www2.opengroup.org/ogsys/catalog/C139	The Open Group	April 18, 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).

Title	Source	Date	Pages	Notes
Governor McDonnell Announces Creation of MACH37, America's Premier Market-Centric Cyber Security Accelerator http://www.commerce.virginia.gov/News/viewRelease.cfm?id=1761	Virginia Secretary of Commerce and Trade	April 11, 2013	N/A	Virginia Governor Bob McDonnell announced the creation of MACH37, America's premier market-centric cyber security 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.
The International Cyber-Security Ecosystem (video lecture) http://smartech.gatech.edu/handle/1853/45450	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 the Information Assurance.
20 Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines - version 4.0 http://www.sans.org/critical-security-controls/	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.
National Cybersecurity Center of Excellence http://csrc.nist.gov/nccoe/	National Institute of Standards and Technology (NIST)	June 29, 2012	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.
Information Security Risk Taking http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1127185	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) http://info.publicintelligence.net/DARPA-ADAMS.pdf	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.

Title	Source	Date	Pages	Notes
At the Forefront of Cyber Security Research http://www.livescience.com/15423-forefront-cyber-security-research-nsf-bts.html	NSF	August 11, 2011	N/A	TRUST is a university and industry consortium that examines cyber security 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 http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf	White House	December 16, 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 http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation	White House Office of Science and Technology Policy	December 6, 2010	10	The Obama Administration released a Memorandum of Understanding signed by the National Institute of Standards and Technology (NIST) 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.
Science of Cyber-Security http://www.fas.org/irp/agency/dod/jason/cyber.pdf	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 http://www.americansecuritychallenge.com/	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.

Related Resources: Other Websites

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

Table 13. Related Resources: Congressional/Government

Name	Source	Notes
Integrated Intelligence Center http://www.cisecurity.org/#	Center for Internet Security	A new unit at the Center for Internet Security is focused on merging cyber and physical security to aid governments in dealing with emerging threats.
Computer Security Resource Center http://csrc.nist.gov/	National Institute of Standards and Technology (NIST)	Links to NIST resources, publications, and computer security groups.
Congressional Cybersecurity Caucus http://cybercaucus.langevin.house.gov/	Led by Representatives Jim Langevin and Mike McCaul.	Provides statistics, news on congressional cyberspace actions, and links to other informational websites.
Cybersecurity and Trustworthiness Projects and Reports http://sites.nationalacademies.org/CSTB/CSTB_059144	Computer Science and Telecommunications Board, National Academy of Sciences	A list of independent and informed reports on cybersecurity and public policy.
Cybersecurity http://www.whitehouse.gov/cybersecurity	White House National Security Council	Links to White House policy statements, key documents, videos, and blog posts.
Cybersecurity http://www.ntia.doc.gov/category/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 http://sites.nationalacademies.org/CSTB/CSTB_045327#Cybersecurity	National Academy of Sciences, Computer Science and Telecommunications Board	A list of independent and informed reports on cybersecurity and public policy.
President's National Security Telecommunications Advisory Committee (NSTAC) http://www.dhs.gov/nstac	U.S. Department of Homeland Security	For over 30 years, the NSTAC has brought together up to 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies. The 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) http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm	U.S. Department of Homeland Security	As the sector-specific agency for the communications and IT sectors, CS&C coordinates national level reporting that is consistent with the National Response Framework (NRF).
U.S. Cyber Command http://www.defense.gov/home/features/2010/0410_cybersec/	U.S. Department of Defense	Links to press releases, fact sheets, speeches, announcements, and videos.
U.S. Cyber-Consequences Unit http://www.usccu.us/	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 14. Related Resources: International Organizations

Name	Source	Notes
Australian Internet Security Initiative http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317	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 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp	Council of Europe	Links to the Convention on Cybercrime treaty, standards, news, and related information.
Cybersecurity Gateway http://groups.itu.int/Default.aspx?alias=groups.itu.int/cybersecurity-gateway	International Telecommunications Union (ITU)	ITU's Global Cybersecurity Agenda (GCA) is the framework for international cooperation with the objective of building synergies and engaging all relevant stakeholders in our collective efforts to build a more secure and safer information society for all.
Cybercrime Legislation - Country Profiles http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp	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 http://www.enisa.europa.eu/	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.)
German Anti-Botnet Initiative http://www.oecd.org/dataoecd/42/50/45509383.pdf	Organisation for Economic Co-operation and Development (OECD) (English-language summary)	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.
International Cyber Security Protection Alliance (ICSPA) https://www.icspa.org/about-us/	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) http://www.ccdcoe.org/	North Atlantic Treaty Organization (NATO)	The Center 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 15. Related Resources: News

Name	Source
Computer Security (Cybersecurity) http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html	*New York Times*
Cybersecurity http://www.nextgov.com/cybersecurity/?oref=ng-nav	NextGov.com
Cyberwarfare and Cybersecurity http://benton.org/taxonomy/term/1193	Benton Foundation
Homeland Security http://homeland.cq.com/hs/news.do	Congressional Quarterly (CQ)
Cybersecurity http://www.homelandsecuritynewswire.com/topics/cybersecurity	Homeland Security News Wire

c11173008

Table 16. Related Resources: Other Associations and Institutions

Name	Notes
Council on Cybersecurity http://www.counciloncybersecurity.org/	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), which 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 http://www.cyberaces.org/	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) http://csis.org/category/topics/technology/cybersecurity	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 http://www.cfr.org/projects/world/cyberconflict-and-cybersecurity-initiative/pr1497	Focuses on the relationship between cyberwar and 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.
Federal Cyber Service from the Scholarship For Service (SFS) https://www.sfs.opm.gov/	SFS is designed to increase and strengthen the cadre of federal information assurance professionals who protect the government's critical information infrastructure. This program provides full scholarships that 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) http://www.thei3p.org/	I3P is a consortium of leading universities, national laboratories and nonprofit institutions dedicated to strengthening the cyber infrastructure of the United States.
Internet Security Alliance (ISA) http://www.isalliance.org/	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) http://www.nascio.org/advocacy/cybersecurity	NASCIO's cybersecurity awareness website. The Resource Guide provides examples of state awareness programs and initiatives.
National Initiative for Cybersecurity Education (NICE) http://csrc.nist.gov/nice/	NICE Attempts to forge a common set of definitions for the cybersecurity workforce.
National Security Cyberspace Institute (NSCI) http://www.nsci-va.org/whitepapers.htm	NSCI provides education, research and analysis services to government, industry, and academic clients to increase cyberspace awareness, interest, knowledge, and capabilities.

c11173008

Name	Notes
U.S. Cyber Challenge (USCC) http://www.uscyberchallenge.org/	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	E-mail
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

c11173008

Legislative Issues	Name/Title	Phone	E-mail
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
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

c11173008