United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2010

CYBERSPACE

United States Faces Challenges in Addressing Global Cybersecurity and Governance

GAO-10-606

July 2010

CYBERSPACE

United States Faces Challenges in Addressing Global Cybersecurity and Governance

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-606, a report to congressional requesters

Why GAO Did This Study

Recent foreign-based intrusions on the computer systems of U.S. federal agencies and commercial companies highlight the vulnerabilities of the interconnected networks that comprise the Internet, as well as the need to adequately address the global security and governance of cyberspace. Federal law and policy give a number of federal entities responsibilities for representing U.S. cyberspace interests abroad, in collaboration with the private sector. More recently, the President appointed a national Cybersecurity Coordinator charged with improving the nation's cybersecurity leadership. GAO was asked to identify (1) significant entities and efforts addressing global cyberspace security and governance issues, (2) U.S. entities responsible for addressing these issues and the extent of their involvement at the international level, and (3) challenges to effective U.S. involvement in global cyberspace security and governance efforts. To do this, GAO analyzed policies, reports, and other documents and interviewed U.S. government and international officials and experts from over 30 organizations.

What GAO Recommends

GAO recommends that the national Cybersecurity Coordinator address challenges including developing a comprehensive national global cyberspace strategy. The national Cybersecurity Coordinator and his staff generally concurred with the recommendations and stated that actions are already being taken.

View GAO-10-606 or key components. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

There are a number of key entities and efforts with significant influence on international cyberspace security and governance. The organizations range from information-sharing forums that are nondecision-making gatherings of experts to private organizations to treaty-based, decision-making bodies founded by countries. Their efforts include those to address topics such as incident response, technical standards, and law enforcement cooperation. For example, the International Organization for Standardization is a nongovernmental organization that develops and publishes international standards, including those related to cybersecurity, through a consensus-based process involving a network of the national standards bodies of 162 countries.

A number of U.S. federal entities have responsibilities for, and are involved in, international cyberspace governance and security efforts. Specifically, the Departments of Commerce, Defense, Homeland Security, Justice, and State, among others, are involved in efforts to develop international standards, formulate cyber-defense policy, facilitate overseas investigations and law enforcement, and represent U.S. interests in international forums. Federal entities have varying roles among organizations and efforts with international influence over cyberspace security and governance, including engaging in bilateral and multilateral relationships with foreign countries, providing personnel to foreign agencies, leading or being a member of a U.S. delegation, coordinating U.S. policy with other U.S. entities through the interagency process, or attending meetings.

The global aspects of cyberspace present key challenges to U.S. policy (see table). Until these challenges are addressed, the United States will be at a disadvantage in promoting its national interests in the realm of cyberspace.

U.S. Challenges in Addressing Global Cybersecurity and Governance

Challenge	Description
Leadership	Providing top-level leadership that can coordinate across federal entities and forge a coherent national approach.
Strategy	Developing a comprehensive national strategy that specifies overarching goals, subordinate objectives, activities to support those objectives, and outcome-oriented performance metrics and time frames.
Coordination	Engaging all key federal entities in order to coordinate policy related to global aspects of cyberspace security and governance.
Standards and policies	Ensuring that international technical standards and polices do not pose unnecessary barriers to U.S. trade.
Incident response	Participating in international cyber-incident response, which includes appropriately sharing information without jeopardizing national security.
Differing law	Investigating and prosecuting transnational cybercrime amid a plurality of laws, varying technical capabilities, and differing priorities.
Norms	Providing models of behavior that shape the policies and activities of countries, such as defining countries' sovereign responsibility regarding the actions of its citizens.

Source: GAO analysis of federal and nonfederal information.

Contents

Figure

Abbreviations

ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
CCIPS	Computer Crime and Intellectual Property Section
CERT	computer emergency response team
CICTE	Inter-American Committee against Terrorism
CITEL	Inter-American Telecommunication Commission
CNCI	Comprehensive National Cybersecurity Initiative
CS&C	Office of Cyber Security and Communication
DHS	Department of Homeland Security
DNS	domain name system
DOC	Department of Commerce
DOJ	Department of Justice
EEB/CIP	Bureau of Economic, Energy, and Business Affairs, International Communications and Information Policy
EUR/RPM	Office of European Security and Political Affairs
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
G8	Group of Eight
HSPD	Homeland Security Presidential Directive
ICANN	Internet Corporation for Assigned Names and Numbers
ICI-IPC	Information and Communications Infrastructure Interagency Policy Committee
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
INL	Bureau of International Narcotics and Law Enforcement Affairs
INR	Bureau of Intelligence and Research
ISO	International Organization for Standardization
ITU	International Telecommunication Union

ITU-D	International Telecommunication Union-Telecommunication Development Sector
ITU-R	International Telecommunication Union-Radiocommunication Sector
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
JCS	Joint Chiefs of Staff
JTC	joint technical committee
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSD	National Security Division
NSPD	National Security Presidential Directive
NTIA	National Telecommunications and Information Administration
OAS	Organization of American States
OASD (GSA)	Office of the Assistant Secretary of Defense for Global Strategic Affairs
OASD (NII)/DOD CIO	Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer
OECD	Organisation for Economic Cooperation and Development
REMJA	Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas
TEL	Telecommunication and Information Working Group
UN	United Nations
USNCB	U.S. National Central Bureau of INTERPOL
USSS	United States Secret Service
USTR	Office of the United States Trade Representative
WPISP	Working Party on Information Security and Privacy
WTO	World Trade Organization

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 2, 2010

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Yvette D. Clarke
Chairwoman
Subcommittee on Emerging Threats, Cybersecurity,
and Science and Technology
Committee on Homeland Security
House of Representatives

The Honorable Kirsten E. Gillibrand
United States Senate

Recent intrusions on U.S. corporations and federal agencies by attackers in foreign countries highlight the threats posed by the worldwide connection of our networks and the need to adequately address global cyberspace security and governance. A multitude of organizations are actively involved in developing international agreements and standards related to the security and governance of cyberspace, and U.S. government and private sector involvement in these organizations and efforts is essential to promoting our national and economic security to the rest of the world.

Cyberspace is the globally interconnected digital information and communications infrastructure. The Internet is a decentralized network of computer networks with no single authority responsible for governing or securing it. Computers attached to the network are subject to the laws and policies of the nation and network where they are physically located, although users from anywhere in the world may be able to post or retrieve information from any particular accessible computer. This complicates Internet governance, as Internet users may be able to use the network to retrieve or post information, such as hate speech, or perform an activity, such as gambling, which is illegal where they are physically located, but not illegal in the country where the computer they are accessing is located.

Our objectives were to identify (1) significant entities and efforts addressing global cyberspace security and governance issues, (2) U.S. entities responsible for addressing cyberspace security and governance

and the extent of their involvement at the international level, and (3) challenges to effective U.S. involvement in global cyberspace security and governance efforts. To identify entities and efforts with significant influence on international cyberspace security and governance, we collected and analyzed documents, such as resolutions, charters, organizational charts, policies, reports, and studies, and conducted structured interviews with relevant federal, private sector, and foreign officials. To identify responsible U.S. entities and their related efforts, we collected, reviewed, and analyzed documents and conducted structured interviews with officials from responsible U.S. departments and agencies, including the Departments of Commerce (DOC), Defense (DOD), Homeland Security (DHS), Justice (DOJ), State, and the Treasury, as well as the Federal Communications Commission (FCC), the United States Agency for International Development (USAID), and the United States Trade Representative (USTR). To determine challenges to effective U.S involvement, we analyzed relevant documentation and the results of structured interviews. Appendix I provides more detail about our objectives, scope, and methodology.

We conducted this performance audit from June 2009 to July 2010, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Internet is a vast network of interconnected networks that is used by governments, businesses, research institutions, and individuals around the world to communicate, engage in commerce, perform research, educate, and entertain. Increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. From its origins in the 1960s as a research project sponsored by the U.S. government, the Internet has grown increasingly important to both American and foreign businesses and consumers, serving as the medium for hundreds of billions of dollars of commerce each year. The Internet has also become an extended information and communications infrastructure, supporting vital services such as power distribution, health care, law enforcement, and national defense.

Today, private industry—including telecommunications companies, cable companies, and Internet service providers—owns and operates the vast majority of the Internet's infrastructure. The various networks that make up the Internet include the national backbone and regional networks, residential Internet access networks, and the networks run by individual businesses or "enterprise" networks. When a user wants to access a Web site or send an e-mail to someone who is connected to the Internet through a different service provider, the data must be transferred between networks. Data travels from a user's device to the Internet through various means, such as coaxial cable, satellite, or wirelessly, to a provider's facility where it is aggregated with other users' traffic. Data cross between networks at Internet exchange points, which can be either hub points where multiple networks exchange data or private interconnection points. At these exchange points, computer systems called routers determine the optimal path for the data to reach their destination. Data travel through the national and regional networks and exchange points around the globe, as necessary, to reach the recipient's Internet service provider and the recipient.

The networks that make up the Internet communicate via standardized rules called protocols. For example, a critical set of protocols, collectively known as the domain name system (DNS), ensures the uniqueness of each e-mail and Web site address. This system links e-mail and Web site addresses with the underlying numerical addresses that computers use to communicate with each other. It translates names into addresses and back again in a process invisible to the end user.

Cyber Threats and Incidents Impact National and Economic Security

The global interconnectivity provided by the Internet allows cyber attackers to easily cross national borders, access vast numbers of victims at the same time, and easily maintain anonymity. Attacks can come from a variety of sources, including criminal groups, hackers, and terrorists. Table 1 lists sources of threats that have been identified by the U.S. intelligence community and others.

Table 1: Sources of Cybersecurity Threats

Threat	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking others, and monetary gain, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as employees who accidentally introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Phishers	Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Sources: GAO analysis based on data from the Director of National Intelligence, Department of Justice, the Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

Different types of cyber threats can use various cyber exploits that may adversely affect computers, software, a network, an agency's operation, an industry, or the Internet itself (see table 2). Groups or individuals may intentionally deploy cyber exploits targeting a specific cyber asset or

attack through the Internet using a virus, worm, or malware with no specific target.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed denial of service	A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vishing	A method of phishing based on voice-over-Internet-Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem, and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

Source: GAO analysis of data from GAO and industry reports.

Recent reports of cyber attacks illustrate that such attacks could have a debilitating impact on national security.

- In May 2007, Estonia was the reported target of a denial-of-service cyber attack with national consequences. The coordinated attack created mass outages of its government and commercial Web sites.[1]

- In March 2008, DOD reported that, in 2007, computer networks operated by DOD, other federal agencies, and defense-related think tanks and contractors were targets of computer network intrusions. Although those responsible were not definitively identified, the attacks appeared to have originated in China.[2]

- In January 2010, it was reported that at least 30 technology companies—most in Silicon Valley, California—were victims of intrusions. The cyber attackers infected computers with hidden programs allowing unauthorized access to files that may have included the companies' computer security systems, crucial corporate data, and software source code.[3]

- In January 2010, a California-based company filed suit alleging that two Chinese companies stole software code and then distributed it to tens of millions of end users as part of Chinese government-sponsored filtering software. The company is seeking more than $2.2 billion dollars. Academic researchers found that portions of the company's software code had been copied and used in initial versions of the Chinese software.[4]

- Based on an 8-month investigation in 2009, university researchers reported that computer systems in India were attacked. The suspected cyberattackers remotely connected to Indian computers using social networks to install bot-nets that infiltrated and infected Indian computers

[1]Computer Emergency Response Team of Estonia, "Malicious Cyber Attacks Against Estonia Come from Abroad," April 29, 2007, and Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference, April 8, 2008.

[2]Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008.*

[3]The New York Times, *Google, Citing Attack, Threatens to Exit China* (Jan. 13, 2010).

[4]The New York Times, *Suit Says 2 Chinese Firms Stole Web-Blocking Code* (Jan. 6, 2010).

with malware. The incidents were reported to have been traced back to an underground espionage organization that was able to steal sensitive national security and defense information.[5]

U.S. Policy Recognizes the Need to Address Global Aspects of Cybersecurity

As threats to cyberspace have persisted and grown and cyberspace has expanded globally, the federal government has developed policies, strategies, and initiatives that recognize the importance of addressing cybersecurity on a global basis. For example, President Obama's *Cyberspace Policy Review* determined that the United States needs a strategy for cybersecurity that brings like-minded nations together on issues such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force.[6] It includes an action to develop U.S. government positions for an international cybersecurity policy and strengthen international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity. The policy review also recommended that the President establish a cybersecurity coordinator position to integrate the government's cybersecurity policies. Subsequently, in December 2009, a Special Assistant to the President and Cybersecurity Coordinator, referred as the Cybersecurity Coordinator in this report, was appointed with responsibility for addressing the recommendations made in the *Cyberspace Policy Review*, including coordinating interagency cybersecurity policies and strategies and developing a comprehensive national strategy to secure the nation's digital infrastructure.

In addition, *The National Strategy to Secure Cyberspace* recognized that securing cyberspace is a global matter due to the interconnectedness of the world's computer systems. Accordingly, it states that securing global cyberspace requires international cooperation to raise awareness, share information, promote security standards, and investigate and prosecute cybercrime.[7] Also, Homeland Security Presidential Directive 7 (HSPD-7) directs DHS to, among other things, develop a comprehensive and

[5]The New York Times, *China Cyber–Spies Target India, Dalai Lama: Report* (Apr. 6, 2010).

[6]The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[7]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

integrated plan outlining goals and initiatives for protecting critical infrastructure that includes a strategy for working with international organizations.[8] The directive also designates the Department of State, in conjunction with the Department of Commerce, DOD, DHS, DOJ, the Department of the Treasury, and other appropriate agencies, to work with foreign countries and international organizations to strengthen the protection of U.S. critical infrastructure and key resources.

Further, while National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), establishing the Comprehensive National Cybersecurity Initiative (CNCI), is focused on safeguarding federal executive branch government information systems, it includes one initiative focused on building an approach that deters interference and attacks in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and nonstate actors.[9] It also recognizes the need to develop an approach to better manage the federal government's global supply chain.

Several Key Entities and Efforts Address Global Cyberspace Security and Governance

There are a number of key entities and efforts whose international activities significantly influence the security and governance of cyberspace. Although these 19 organizations, listed in table 3, do not represent all international cyber-related entities and efforts, they were consistently identified as key by the organizations and experts we interviewed. The organizations range from information-sharing forums that are nondecision-making gatherings of experts to private organizations to treaty-based, decision-making bodies founded by countries. Their efforts include those to address topics such as incident response, technical standards, and law enforcement cooperation. These entities have reported ongoing initiatives that involve governments and private industry stakeholders to address a broad set of topics, such as implementation of incident response mechanisms, the development of technical standards, the facilitation of criminal investigations, and the creation of international policies related to information technology and critical infrastructure.

[8]The White House, *Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: Dec. 17, 2003).

[9]The White House, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (Washington, D.C.: Jan. 8, 2008).

Table 3: Key Entities and Efforts with Significant Influence on International Cyberspace Security and Governance

Asia-Pacific Economic Cooperation	International Electrotechnical Commission	Meridian
Association of Southeast Asian Nations	International Organization for Standardization	North Atlantic Treaty Organization
Council of Europe	International Telecommunication Union	Organization of American States
European Union	Internet Corporation for Assigned Names and Numbers	Organisation for Economic Cooperation and Development
Forum of Incident Response and Security Teams	Internet Engineering Task Force	United Nations
Group of Eight	Internet Governance Forum	
Institute of Electrical and Electronic Engineers	INTERPOL	

Source: GAO analysis of data provided by U.S. and foreign governmental agencies and the private sector.

Asia-Pacific Economic Cooperation

Asia-Pacific Economic Cooperation (APEC) is a cooperative economic and trade forum designed to promote economic growth and cooperation among 21 countries from the Asia-Pacific region.[10] APEC's Telecommunication and Information Working Group (TEL) is to support security efforts associated with the information infrastructure of member countries through activities designed to strengthen effective incident response capabilities, develop information security guidelines, combat cybercrime, monitor security implications of emerging technologies, and foster international cooperation on cybersecurity. According to APEC, the working group has pursued some of these activities by collaborating with other international organizations, such as the Association of Southeast Asian Nations, the International Telecommunication Union, and the Organisation for Economic Cooperation and Development.

Association of Southeast Asian Nations

Association of Southeast Asian Nations (ASEAN) is an economic and security cooperative comprised of 10 member nations from Southeast Asia.[11] According to the 2009-2015 *Roadmap for an ASEAN Community*, it seeks to combat transnational cybercrime by fostering cooperation among member-nations' law enforcement agencies and promoting the adoption of

[10]Member countries include: Australia; Brunei Darussalam; Canada; Chile; the People's Republic of China; Hong Kong, China; Indonesia; Japan; the Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Republic of the Philippines; the Russian Federation; Singapore; Chinese Taipei; Thailand; the United States; and Vietnam.

[11]ASEAN's 10 member nations are Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam.

cybercrime legislation.[12] In addition, the road map calls for activities to develop information infrastructure and expand computer emergency response teams (CERT) and associated drills to all ASEAN partners.

Council of Europe

The Council of Europe is an organization of 47 member countries founded in 1949 to develop common and democratic principles for the protection of individuals. In 2001, the council adopted a Convention on Cybercrime to improve international cooperation in combating actions directed against the confidentiality, integrity, and availability of computer systems, networks, and data. This convention identified agreed-upon cyber-related activities that should be deemed criminal acts in countries' domestic law. These acts included illegal access to a computer system, computer-related fraud, activities involving child pornography, and copyright infringement. The U.S. Senate ratified this convention in August 2006. The Council of Europe also sponsors training and conferences to address cybersecurity issues such as its 2009 joint conference with the Organization of American States/Inter-American Committee against Terrorism, which focused on ways in which the Internet is misused by terrorist organizations and their supporters.

European Union

The European Union is an economic and political partnership among 27 European countries.[13] Subcomponents of its executive body—the European Commission—are to engage in cybersecurity activities designed to improve (1) preparedness and prevention, (2) detection and response, (3) mitigation and recovery, (4) international cooperation, and (5) criteria for European critical infrastructure in the information communication technology sector. European Commission officials stated that, in the future, the European Commission will prioritize international engagement involving mutual assistance, recovery efforts, and crisis management.

In addition, the European Commission formed the European Network and Information Security Agency (ENISA), an independent European agency created to enhance the capability of its members to address and respond to network and information security problems. Established in 2004,

[12]ASEAN Secretariat, *Roadmap for an ASEAN Community 2009-2015* (Jakarta: April 2009).

[13]Member countries include: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

ENISA's international outreach is to primarily focus on information infrastructure protection and resilience, awareness raising, and the exchange of information among its members. Officials stated that they anticipate performing greater international outreach outside of Europe beginning in 2012.

Several independent organizations within Europe develop technical standards. The European Committee for Standardization is to work to remove trade barriers for European industry and provide a platform for the development of European standards and technical specifications. The European Committee for Electrotechnical Standardization is a not-for-profit technical organization that is responsible for preparing voluntary electrotechnical standards for electrical and electronic goods and services in the European market. The European Telecommunications Standards Institute is also a not-for-profit organization that is responsible for producing globally applicable standards for information and communications technologies including those supporting the Internet.

Forum of Incident Response and Security Teams

Forum of Incident Response and Security Teams (FIRST) is an international confederation of individual CERTs that work together to share technical and security incident information. It includes over 220 members from 42 countries. The members' incident response teams represent government, law enforcement, academia, the private sector, and other organizations. FIRST's steering committee is responsible for its general operating policy, procedures, and other matters affecting the organization. The steering committee also selects the Secretariat, the coordinator of meetings and workshops, and the administrator for data and communications.

According to FIRST, it has also worked with multiple international standards organizations to develop standards for cybersecurity and incident management and response. In addition, FIRST uses the Common Vulnerability Scoring System as a standard method for rating information technology vulnerabilities, which helps when communicating vulnerabilities and their properties to others.

Group of Eight

The Group of Eight (G8) is an international forum that includes the governments of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. The G8's cybersecurity efforts are directed by the G8 Subgroup on High-Tech Crime, which seeks to prevent, investigate, and prosecute crimes involving computers, networked communications, and other new technologies. In 1997, the subgroup created the 24-7 High-Tech Crime Point-of-Contact Network, which allows

	law enforcement officials from countries—including those from outside the G8—to quickly contact their counterparts in other participating nations for assistance with cybercrime investigations. The network is to supplement traditional methods of obtaining law enforcement assistance. In 2004, the Subgroup on High-Tech Crime also developed a best practices guide for network security to assist network operators and system administrators when responding to computer incidents.
Institute of Electrical and Electronic Engineers	The Institute of Electrical and Electronic Engineers (IEEE) is a professional association focused on electrical and computer sciences, engineering, and related disciplines. Its cybersecurity-related activities include the development of technical standards through the IEEE Standards Association, which follows consensus-based standards development processes. For example, IEEE standards include 802.11, an internationally recognized standard that addresses encryption and wireless networking. In addition, according to its reports, the IEEE Standards Association has been involved with the U.S. National Institute of Standards and Technology (NIST) to draft cybersecurity standards for electric utility control systems.
International Electrotechnical Commission	The International Electrotechnical Commission (IEC) prepares and publishes international standards for electrical, electronic, and related technologies. Its membership includes national committees from over 70 nations, which are comprised of representatives from each country's public and private sectors. The IEC and the International Organization for Standardization (ISO), through a joint technical committee (JTC), have developed information security standards for all types of organizations, including commercial enterprises, government agencies, and not-for-profit organizations. For example, ISO/IEC 27001:2005 addresses the development and maintenance of information security management systems and the security controls that protect information assets. According to the standard, ISO/IEC JTC 1 developed this international standard to be applicable to all organizations regardless of size.
ISO	ISO is a nongovernmental organization that develops and publishes international standards through a consensus-based process involving a network of the national standards institutes of 162 countries with a Central Secretariat in Geneva, Switzerland, supporting the process. Its standards include those for traditional activities such as agriculture and construction, as well as those for the latest in information and communication technology. As previously mentioned, the ISO is a part of the ISO/IEC JTC 1.

The International Telecommunication Union

The International Telecommunication Union (ITU) is a United Nations (UN) agency whose mission includes developing technical standards, allocating the radio spectrum, and providing technical assistance and capacity-building to developing countries. According to ITU, three sectors carry out these missions by promoting recommendations: the ITU-Telecommunication Standardization Sector (ITU-T), the ITU-Radiocommunication Sector (ITU-R), and the ITU-Telecommunication Development Sector (ITU-D). In addition, the ITU General-Secretariat provides top-level leadership to ensure that institutional strategies are harmonized across all sectors. ITU members include delegations from 191 nations, as well as more than 700 members from the private sector.

The ITU has also developed technical standards for security and, more recently, engaged in other cybersecurity activities. For example, ITU-T has established a study group for telecommunications security to focus on developing standards and recommendations associated with network and information security, application security, and identity management. Similarly, ITU-D, through its members' efforts, prepared a report on cybersecurity best practices for countries seeking to organize national cybersecurity efforts. While this effort was underway, the ITU General-Secretariat separately issued a Global Cybersecurity Agenda (GCA) designed to promote a comprehensive and coordinated international approach to cybersecurity across all ITU sectors. The GCA has five specific focus areas: legal measures, technical and procedural measures, organizational structures, capacity-building, and international cooperation. In addition, the ITU Secretary General signed a memorandum of understanding with the International Multilateral Partnership Against Cyber Threats that is to establish an operations center to coordinate incident response and to provide cyber threat information to member countries and the private sector.[14]

Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is the private, not-for-profit U.S. corporation whose primary function is the coordination of the technical management of the Internet's domain name and addressing system. According to ICANN officials, the corporation is overseen by a board of directors composed of 21 representatives, including 15 voting members and 6 nonvoting liaisons. It signed an Affirmation of Commitments with the Department of Commerce in

[14]The relationship between ITU and the International Multilateral Partnership Against Cyber Threats is managed by ITU-D.

September 2009, which, according to department officials, completed the transition of the technical management of the DNS to a private-sector led, multistakeholder model that is intended to ensure accountability and transparency in its decision-making with the goal of protecting the interests of global Internet users. ICANN is to facilitate DNS policy development through a bottom-up process involving the diverse interests of generic and country code top-level domain registries, domain name registrars, the regional Internet registries, the technical community, business and individual Internet users, and governments. According to ICANN officials, it also performs the Internet Assigned Names Authority functions under contract to the Department of Commerce. The Internet Assigned Names Authority's functions consist of several interdependent Internet management responsibilities, including coordination of the assignment of technical protocol parameters, performance of administrative functions associated with root zone management, and the allocation of Internet numbering resources.

Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is a technical standards-setting body responsible for developing and maintaining the Internet's core standards, including the DNS protocol and its security extensions and the current and next-generation versions of the Internet Protocol. According to government officials, the core standards the IETF develops define, on a basic level, how the Internet operates and what functions it is capable of performing. It is a voluntary, consensus-based standards body, whose participants include network operators, academics, and representatives of government and industry, among others. Much of IETF's work is conducted via e-mail lists, although it does host three meetings at locations around the world each year.

The Internet Governance Forum

The 2005 World Summit on the Information Society's Tunis Agenda mandated that the UN Secretary-General create the Internet Governance Forum (IGF) as a multistakeholder venue to discuss public policy issues related to key elements of Internet governance. According to a recognized expert, the IGF's broad membership and emphasis on information exchange enable it to serve as a uniquely important forum for foreign governments, the private sector, civil society organizations, and individuals to engage in open discussion without being preoccupied with advocating a particular policy outcome. Although the annual meetings do not directly result in standards, recommendations, or binding agreements, ideas generated by IGF can contribute to outcome-oriented efforts at other international organizations.

INTERPOL	INTERPOL, the world's largest international police organization, was created to facilitate cross-border police cooperation. It collects, stores, analyzes, and shares information related to cybercrime between its 188 member countries through its global police communications system. It is also responsible for coordinating operational resources such as computer forensic analysis in support of cybercrime investigations. Further, INTERPOL has a network of investigators in national computer crime units to help law enforcement seize digital evidence as quickly as possible and facilitate cooperation when a cyber attack involves multiple jurisdictions. To develop strategies for emerging cybercrime methods, it assembles groups of experts into regional working groups that harness the regional expertise available in Europe, Asia, the Americas, the Middle East, and North Africa. The working party activities are to include sharing information on regional cybercrime trends, enhancing cooperation among the member countries, and developing educational materials for law enforcement.
Meridian	Founded in 2005, the Meridian Conference and Process aims to exchange ideas and initiate actions for government-to-government cooperation on critical information infrastructure protection issues globally. An annual conference and interim activities are held each year to help build trust and establish relationships within the membership to facilitate sharing of experiences and good practices on critical information infrastructure protection from around the world. Participation in the Meridian Process is open to all countries and aimed at senior government policy-makers. DHS's National Protection and Programs Directorate's Office of Cyber Security and Communication hosted the 2009 Meridian Conference, which brought together more than 100 participants from 40 countries. The conference allowed participants to explore the benefits of and opportunities for cooperation between governments and share best practices. Key U.S. cybersecurity leaders from DHS and the White House engaged with conference delegates and shared views on U.S. cybersecurity priorities. The Meridian Process also seeks to advance collaborative efforts on specific topics such as control systems security.
North Atlantic Treaty Organization	The North Atlantic Treaty Organization (NATO) is an alliance of 28 countries from North America and Europe.[15] NATO approved a Cyber

[15]NATO's member countries are: Albania, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, the United Kingdom, and the United States.

Defense Policy in January 2008 to provide direction to its member nations to protect key information systems and support efforts to counter cyber attacks. Specifically, the policy establishes the Cyber Defense Management Authority, which has authority for managing cyber defense crises, to include directing the NATO Computer Incident Response Capability. NATO also encourages the creation of state-sponsored cyber-defense authorities to exchange information, define the scope of mutual support in the event of an identified cyber incident, and to identify communication and information systems that handle information deemed critical to the alliance.

Organization of American States

The Organization of American States (OAS) is an intergovernmental organization comprised of 34 independent nations in North, Central, and South America, as well as island nations in the Caribbean.[16] In 2004, the OAS member states adopted the Inter-American Comprehensive Strategy for Cybersecurity. The strategy identifies cybersecurity as an emerging threat to OAS member states and requires three OAS entities to take action to address different aspects of cybersecurity. Specifically, the strategy directs the Inter-American Committee against Terrorism (CICTE) to develop plans for the creation of a hemisphere-wide, 24-hours-per-day, 7-days-per-week network of Computer Security Incident Response Teams. In addition, the strategy directs the Inter-American Telecommunication Commission (CITEL) to evaluate existing technical cybersecurity standards, recommend the adoption of particularly important cybersecurity standards, and identify obstacles to implementing those cybersecurity standards within the Americas. Finally, the strategy directs the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA), through the Group of Government Experts on Cyber-Crime, to provide technical assistance to member states in drafting and enacting effective computer crime laws to protect information systems and facilitate investigations and prosecutions.

[16]OAS member countries are: Antigua and Barbuda, Argentina, the Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, the Grenadines, Guatemala, Guyana, Haiti, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, St. Kitts and Nevis, Saint Lucia, Saint Vincent, Suriname, Trinidad and Tobago, the United States, Uruguay, and Venezuela.

Organisation for Economic Cooperation and Development

The Organisation for Economic Cooperation and Development (OECD) is an intergovernmental organization composed of 31 democratic countries.[17] Member countries' governments can compare policy experiences, seek answers to common problems, identify best practices, and coordinate domestic and international policies. The OECD Working Party on Information Security and Privacy (WPISP) uses a consensus-based process to develop policy options to address the security and privacy implications of the growing use of information and communication technologies. In addition to developing policy analysis, OECD is responsible for making recommendations designed to improve the security and privacy of its member countries. For example, in 2008, the OECD Council adopted a recommendation calling for member countries to cooperate among themselves and with the private sector to improve the protection of critical information infrastructure. Specifically, the recommendations called for bilateral and multilateral sharing of best practices, development of common understandings of cross-border interdependencies and vulnerabilities, identification of national agencies involved in critical information infrastructure protection, acknowledgment of the value of international watch and warning networks, and international cooperation on cyber research and development.

UN

The UN is an international organization with 192 member countries founded in 1945 and chartered to maintain international peace and security, develop friendly relations among countries, and promote social progress, better living standards, and human rights. The General Assembly, which provides a forum for discussing and adopting resolutions on cyberspace-related issues and raising international cybersecurity awareness, is the UN's chief deliberative, policymaking, and representative body. Other organizational entities within the UN, such as the Office on Drugs and Crime, are additional forums where member countries can discuss approaches for transnational issues, including cybercrime.

[17]OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. In addition, in May 2010, Estonia, Israel, and Slovenia were invited by OECD countries to join the organization.

U.S. Government Entities Are Involved with Multiple Global Cyberspace Security and Governance Efforts

Multiple U.S. government entities participate in the formulation, coordination, implementation, and oversight of international efforts that can impact cyberspace security and governance. These efforts are authorized by statutes, presidential directives, and national policies. Federal entities' involvement in these efforts ranges from engaging in bilateral and multilateral relationships with foreign countries to providing personnel to foreign agencies to leading or being a member of a U.S. delegation to attending meetings.

National Security Council

The National Security Council (NSC) is the principal forum for considering national security and foreign policy matters that require presidential involvement. The NSC was established by the National Security Act of 1947 and subsequently placed within the Executive Office of the President. Presidential Policy Directive-1, signed in February 2009, directs multiple federal entities to participate in NSC meetings and established interagency policy committees to serve as the main mechanisms for coordination of national security policy. The committees are designed to provide policy analysis for consideration by more senior committees within the NSC system and ensure timely responses by the President. According to DOD officials, the NSC approved an Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) in March 2009. Officials further stated that the ICI-IPC subsequently approved a subcommittee to focus on international cyberspace policy efforts (International Sub-IPC). Officials from the Departments of Commerce, Defense, Homeland Security, Justice, State, and the Treasury, as well as officials from the Office of the United States Trade Representative and the Federal Communications Commission stated that they participate in the International Sub-IPC, where they coordinate international cyberspace-related policy efforts.

Department of Commerce

The Department of Commerce's (DOC) mission is to foster, promote, and develop the foreign and domestic commerce of the United States. It is responsible under HSPD-7, in coordination with other federal and nonfederal entities, for improving technology for cyber systems and promoting critical infrastructure efforts, including using its authority under the Defense Production Act. Two of the department's subcomponents are responsible for activities that can impact international efforts related to cyberspace security and governance. The National Telecommunications and Information Administration (NTIA) is to serve as

the principal presidential adviser on information policy and telecommunications issues. In addition, NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. According to NIST officials, it carries out these responsibilities, in part, with the American National Standards Institute (ANSI), a U.S. organization that is responsible for coordinating and promoting voluntary consensus standards and information-sharing to minimize overlap and duplication of U.S. standards-related efforts.[18] Department of Commerce officials also stated that the department participates in the activities of the International Sub-IPC. NTIA and NIST officials provided descriptions of their efforts, which we summarized in table 4.

Table 4: Department of Commerce's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of effort
NTIA	• Oversees the Internet Assigned Names Authority contract, and negotiated the Affirmation of Commitments signed between the U.S. government and ICANN in September 2009. NTIA also represents the U.S. government on ICANN's Government Advisory Committee. • Participates in ITU-T study group efforts (cybersecurity standards, promotion of neutral policy-related outputs as appropriate) as a substantive expert member of U.S. delegations. • Participates in ITU-D study group efforts (national best-practices guidelines, tools to promote a culture of cybersecurity, and cybersecurity self-assessment tools) as an expert member of U.S. delegations. • Participates in ITU-R study group efforts (spectrum management) as an expert member of U.S. delegations. • Has participated in technical, policy, and regulatory capacity-building efforts in Latin America and the Caribbean through efforts in OAS-CITEL as an expert member of U.S. delegations. • Participates in technical, policy, and regulatory capacity-building efforts in Latin America through efforts in OAS-CICTE as an expert member of its workshops and through efforts supporting its work in global cyber incident response team development.

[18]A December 2000 memorandum of understanding between ANSI and NIST establishes the organizations' agreement on a unified national approach to developing national and international standards. The memorandum states that ANSI is the representative of U.S. interests in international standards-developing organizations.

Agency/component	Description of effort
	• Participates in policy and regulatory training sessions through specialized U.S. Telecommunications Training Institute training activities. • Participates in APEC-TEL regarding issues such as cybersecurity and child online safety. • Oversees the implementation of Domain Name System Security Extensions at the authoritative root zone, as well as its implementation within the US and EDU top-level domains. • Joined OECD WPISP's Volunteer Group on Cybersecurity Strategies which was created in March 2010 to monitor potential overlaps with other intergovernmental cybersecurity forums. • Participates in IETF meetings to track DNS and Internet Protocol-related activities. • Participates in IGF meetings. • Has participated in technical infrastructure capacity-building efforts (such as for Central Asia and Eastern Africa). • Participates in the International Sub-IPC.
NIST	• Chairs (since as early as 2002) and participates in multiple U.S. technical advisory groups to JTC-1 that have developed or are developing standards related to security evaluation techniques, identity management, identification card and smart card interoperability, cloud computing, biometrics, and cryptography. • Participates in ITU-T study group efforts via the joint standards development project with ISO-IEC JTC-1. • Serves as editor and area director while contributing to IETF standards efforts, including multiple efforts related to Internet Protocol version 6. • Serves as editor and otherwise contributes to IEEE 802. • Provides guidance to organizations for implementing wireless networks standards.

Source: GAO analysis of Department of Commerce data.

DOD

DOD provides the military forces needed to protect the security of the United States. As part of its mission, DOD is responsible for protecting and defending its networks, including independently establishing bilateral relationships with foreign military and other international partners to share computer vulnerability data and coordinate activities and operations. As a federal department with cyber expertise, DOD is included by HSPD-7 among the departments that are to collaborate with DHS to secure cyberspace. Under these authorities, multiple subcomponents within the department are responsible for cyberspace activities related to strategy, policy, plans, and operations. The Office of the Assistant Secretary of Defense for Global Strategic Affairs (OASD (GSA)) is the primary policy organization within DOD responsible for formulating the department's international cyberspace policies. The Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (OASD(NII)/DOD CIO) is to develop and coordinate information-sharing relationships with international military partners to support computer network defense operations. The Joint Staff J-5 is responsible for translating national policy into joint doctrine for DOD's

combatant commands and represents the Joint Chiefs of Staff (JCS) at the ICI-IPC. DOD officials also stated that the department has a role in the activities of the International Sub-IPC. DOD officials provided descriptions of their efforts, which we summarized in table 5.

Table 5: DOD's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of effort
OASD (GSA)	• Develops DOD strategy for international cyberspace engagement and coordinates intra-agency cyber activities for the Secretary and Deputy Secretary of Defense. • Supports NATO cyberspace policy development. • Participates in ITU-T and ITU-D study group efforts (cybersecurity standards, national best-practices guidelines, tools to promote a culture of cybersecurity, and cybersecurity self-assessment tools) as a member of U.S. delegations. • Participate in UN General Assembly proceedings as subject matter expert in U.S. delegations. • Participates in an intra-agency working group related to ICANN. • Develops bilateral and multilateral agreements regarding military cooperation for cyberspace operations. • Provides policy guidance to other U.S. agencies participating in international efforts via the International Sub-IPC.
OASD(NII)/DOD CIO	• Leads the International Information Assurance Program, which develops and manages cyber-related bilateral and multilateral data sharing relationships with foreign military partners. • Represents the United States at the NATO C3 Board that approves the NATO Cyber Defense Policy and directs policy implementation via the Cyber Defense Management Board. • Sponsors the biannual International Cyber Defense Workshop, which provides technical security training to military and civilian information assurance specialists and computer security practitioners on topics including computer network defense, response and analysis, and computing forensics. • Provides technical expertise and guidance to other U.S. agencies participating in international efforts via the International Sub-IPC.
JCS	• Maintains Joint Staff country desk officers to liaise with foreign military counterparts in coordination with Defense Attachés and the Department of State. • Provides liaison officers to the UN Military mission. • Develops and provides professional military education with respect to joint military doctrine, including cyberspace operations, to allied nations. • Represents the JCS and provides guidance to other U.S. agencies participating in international efforts via the International Sub-IPC.

Source: GAO analysis of DOD data.

DHS

DHS is responsible for preventing and deterring terrorist attacks and protecting against and responding to other threats and hazards within the United States, including with regard to key resources and critical infrastructure. Federal law and policy also tasks DHS with critical infrastructure protection responsibilities that include strengthening international cyberspace security in conjunction with other federal

agencies, international organizations, and industry. Multiple DHS subcomponents conduct activities that are related to cyberspace security and governance. According to DHS officials, the Office of Cyber Security and Communications (CS&C) is responsible for, among other things, building and maintaining a national cyberspace response system, implementing a cyber-risk management program for protection of critical infrastructure, and planning for and providing national security and emergency preparedness communications to the federal government. DHS officials also stated that the department has a role in the activities of the International Sub-IPC. DHS's United States Secret Service (USSS) is responsible for investigating crimes related to U.S. financial infrastructure, including computer fraud, cybercrime, and other types of electronic crimes. DHS officials provided descriptions of their efforts, which we summarized in table 6.

Table 6: DHS's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of efforts
CS&C	• Participates in ITU-T's cybersecurity and telecommunications standards study group efforts as a member of U.S. delegations. • Participates in ITU-D's cybersecurity capacity-building study group efforts (such as national cybersecurity best-practices guides and cybersecurity self-assessment tools) as a member of U.S. delegations. • Engages multi-national companies to develop key practices that mitigate risk to the global supply chain. • Co-sponsors an international academic working group reviewing international standards for information assurance education. • Conducts large-scale cybersecurity exercises, such as Cyber Storm, with international partners to improve incident response and coordination capabilities. • Participates in FIRST. • Coordinates the development of incident response standard operating procedures for the International Watch and Warning Network, a government-to-government forum. The network was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities, and enhancing global cyber situational awareness and incident response capabilities. • Serves on the Steering Committee for the Meridian Process and serves as chair of the Meridian Process Control Systems Information Exchange. • Serves as the Deputy Co-Convener of the cybersecurity-focused biannual meetings of APEC-TEL's Security and Prosperity Steering Group; promotes cybersecurity exercises, awareness raising, and other topics by convening and participating in APEC-TEL workshops; directly participates in APEC-TEL meetings as a member of U.S. delegations.

Agency/component	Description of efforts
	• Advises on the OECD's WPISP efforts as a member of U.S. delegations. • Participates in OAS-CICTE efforts to advance cybersecurity and develop cyber incident response teams across the hemisphere and promote regional capacity-building. • Participates in OAS-CITEL cybersecurity standards efforts as a member via the U.S. mission (including workplan development and increasing the level of training). • Participated in the 2009 Organization for Security and Co-operation in Europe meeting focused on cybersecurity. • Engages in bilateral and multilateral relationships with foreign countries including information sharing on issues of mutual concern and operations; exchanging good practices; collaborating on the development of mitigation measures; and coordination of watch, warning, and incident response efforts. • Provides cybersecurity-related training to developing nations at the U.S. Telecommunication and Training Institute. • Provides subject matter expertise to NATO's Civil Communications Planning Committee on programs/activities that address cybersecurity. • Participates in international efforts via the International Sub-IPC. • Provides control systems security training to developed and developing nations.
USSS	• Participates in OAS-CICTE efforts. • Participates in OAS-REMJA efforts. • Assigns USSS personnel to DOJ to coordinate criminal investigations with INTERPOL. • Investigates transnational cybercrimes using electronic crimes special agents assigned both domestically and internationally, including through the European Electronic Crimes Task Force. • Provides training to International Law Enforcement Academies and forensics training to European partners through the European Electronic Crimes Task Force.

Source: GAO analysis of DHS data.

DOJ

DOJ is the chief law enforcement agency of the U.S. government and is responsible for prosecuting violations of cyber-related laws such as the Computer Fraud and Abuse Act. HSPD-7 also directs DOJ to work with DHS in efforts to investigate and prosecute threats to and attacks against cyberspace. Further, the directive instructs DOJ, and other federal agencies, to work with foreign countries and international organizations to strengthen critical infrastructure and key resources of the United States. DOJ officials also stated that the department has a role in the activities of the International Sub-IPC.

According to DOJ officials, multiple DOJ subcomponents conduct activities that can impact international efforts related to cyberspace security and governance. For example, DOJ's Criminal Division, through the Computer Crime and Intellectual Property Section (CCIPS), is responsible for prosecuting U.S. citizens and foreign nationals who commit electronic crime. CCIPS also provides international training on cybercrime and participates in a number of international organizations

addressing cybercrime. The Federal Bureau of Investigation's (FBI) Cyber Division is the lead federal agency for investigating cybercrime, including criminal intrusions, online child protection, intellectual property protection, and identity theft. In addition, the FBI operates the -National Cyber Investigative Joint Task Force that includes intelligence and law enforcement agencies and is tasked with investigating, predicting, and preventing cyber terrorism, cyber espionage, and cybercrime. DOJ's National Security Division's (NSD) primary mission is counterterrorism and protecting against other threats to national security, and it is responsible for coordinating efforts between the U.S. intelligence community and prosecutors and law enforcement agencies. The U.S. National Central Bureau of INTERPOL (USNCB) represents the United States as an INTERPOL member and serves as a point of contact for U.S. federal, state, local, and tribal law enforcement for the international exchange of information for criminal investigations. DOJ officials provided descriptions of their international efforts related to cyberspace security and governance, which we summarized in table 7.

Table 7: DOJ's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of efforts
CCIPS	• Prosecutes U.S. citizens and foreign nationals who commit electronic crime. • Leads U.S. efforts at the G8 Subgroup on High-Tech Crime, including management of the 24-7 High-Tech Crime Points-of-Contact Network. • Chairs the OAS-REMJA Experts Group and participates in training programs related to investigating and prosecuting cyber crimes. • Participates in providing training programs to APEC and ASEAN member states related to investigating and prosecuting cyber crimes. • Provides training to African countries related to cybercrime, including cooperative assistance with legislative drafting and investigative training programs, in connection with the African Union, Economic Community of West African States, Common Market for Eastern and Southern Africa, and Organisation International de la Francophonie. • Monitors ITU-D study group efforts and GCA activities related to cybercrime. • Chairs the implementation committee of, and provides training related to, the Council of Europe's Convention on Cybercrime. • Participates in OECD's WPISP meetings. • Participates in the Organization for Security and Co-operation in Europe meetings. • Participates in UN General Assembly proceedings.

Agency/component	Description of efforts
	• Participates in the UN Crime Congress and Crime Commission negotiations. • Interacts with the European Union's Freedom, Security, and Justice directorate regarding multiple cybercrime related topics, such as the Budapest Convention on Cybercrime, international cybercrime training, and policy issues associated with ICANN. • Participates, in coordination with the FBI and other government agencies, in efforts to ensure ICANN management is aware of law enforcement and public safety needs related to preservation of records. • Has provided law enforcement training to CERT organizations, including FIRST. • Establishes bilateral and multilateral relationships with foreign countries to cooperate on cybercrime investigations and cyber-related training. • Participates in U.S. foreign policy efforts related to cyberspace issues including free speech rights and jurisdictional questions. • Proposes, or comments on proposals for, legislation affecting international cybercrime; on request, critiques other countries' draft cybercrime statutes. • Runs interagency meetings to coordinate international cybercrime training. • Provides training and emergency assistance to U.S. and foreign agencies, including INTERPOL, for obtaining electronic evidence from foreign countries. • Provides policy guidance to other U.S. agencies participating in international efforts, via the International Sub-IPC.
FBI Cyber Division	• Investigates violations of U.S. laws related to cybercrime. • Posts legal attachés to U.S. embassies to serve as the FBI's representatives. • Establishes bilateral and multilateral relationships with foreign countries to cooperate on cybercrime investigations; chairs the Strategic Alliance Cyber Crime Working Group, a multilateral effort with close U.S. allies to improve law enforcement cooperation. • Leads an international task force related to the Innocent Images National Initiative designed to combat the production, distribution, and possession of child pornography and online predators. • Provides agency personnel to foreign law enforcement agencies to provide support to cybersecurity-related investigations and foster law enforcement relations. • Leads ICANN international meetings and Regional Internet Registry meetings to ensure Internet Service Providers and Regional Internet Registries are aware of law enforcement requirements with regard to the DNS. Introduced, along with the UK Serious Organized Crime Agency, LE Registrar Accreditation Agreement and Due Diligence proposal before the ICANN Governmental Advisory Board and Board of Directors at the ICANN meeting in Seoul, Korea. • Provides cybercrime investigation training to foreign students via International Law Enforcement Academies.
NSD	• Participating in Cyber Storm III, a planned large-scale cybersecurity exercises with international partners to improve incident response and coordination capabilities. • Consulted on white paper regarding the Global Internet Freedom Initiative. • Participates in UN Counterterrorism Implementation Task Force workshops on legal and technical aspects of countering terrorist use of the Internet. • Participates in the International Sub-IPC.
USNCB	• Serves as U.S. liaison to INTERPOL.

Source: GAO analysis of DOJ data.

Department of State

As the lead U.S. agency with responsibility for foreign affairs, the Department of State has a variety of duties relating to cyberspace. For example, it is responsible for the formulation, coordination, and oversight of foreign policy related to international communications and information policy, including exercising primary authority for the determination of U.S. positions and the conduct of U.S. participation in negotiations with foreign governments and international bodies. It is also responsible for coordination and oversight with respect to all major science and technology agreements. In addition, under the 2003 *National Strategy to Secure Cyberspace*, the Department of State is to lead federal efforts to enhance international cyberspace security cooperation. Under HSPD-7, the department is also to work collaboratively with DHS in efforts to secure cyberspace. Further, according to officials, the department has a role in CNCI efforts and the activities of the International Sub-IPC. Department officials further stated that the department focuses on engaging countries, bilaterally and multilaterally, on a range of cyberspace issues.

To fulfill the department's lead responsibility, a number of Department of State entities are given roles. For example, the Bureau of Economic, Energy, and Business Affairs, International Communications and Information Policy (EEB/CIP), is responsible for international telecommunications and information policy. In addition, the Bureau of Intelligence and Research (INR), Office of Cyber Affairs, is responsible for providing intelligence analysis and coordinating international outreach on cybersecurity issues. The Bureau of International Narcotics and Law Enforcement Affairs (INL) is responsible for coordinating policy and programs to combat cybercrime. Finally, the Office of European Security and Political Affairs (EUR/RPM) develops and coordinates policy on U.S. security interests in Europe. Department officials provided descriptions of their bureaus' specific international efforts, which we summarized in table 8. During the course of our work, Department of State officials stated that their department had initiated an internal reorganization that would determine how its cybersecurity related activities will be coordinated; however, the reorganization had not yet occurred.

Table 8: Department of State's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of efforts
EEB/CIP	• Leads the coordination and development of U.S. positions for ITU meetings, including the ITU Plenipotentiary Conference, World Telecommunication Development Conference, World Telecommunication Standardization Assembly, and World Radiocommunication Conference. • Leads U.S. delegations to ITU-T, including study group efforts focused on developing cybersecurity standards, cable transmission standards, next generation networks, and cybersecurity. • Leads U.S. delegations to ITU-D and chaired study group efforts focused on national best-practices guides and cybersecurity self-assessment tools. • Participates in ITU-R study group efforts related to cybersecurity. • Provides input into the ITU-GCA through the annual meeting of the ITU Council; participated in the Group of Experts that helped identify global cybersecurity issues and recommend activities for ITU involvement. • Holds an annual Information Society Dialogue with the European Commission to exchange information on telecommunications and information and communications technology developments. • Participate in IGF meetings as moderators, panelists, and attendees. • Co-Chairs with the Bureau of Democracy, Human Rights, and Labor, the NetFreedom Task Force whose goal is to promote the free flow of information and freedom of expression on the Internet. • Leads U.S. delegations to biennial meetings of the APEC-TEL's Security and Prosperity Steering Group. • Leads U.S. delegations to OECD's WPISP meetings to develop policy options to sustain trust, information security, and privacy. • Leads U.S. delegations to OAS-CITEL meetings to discuss regional positions on issues pending before the ITU, including cybersecurity. • Engages in bilateral and multilateral relationships with foreign countries to address a range of cybersecurity issues. • Participates in Sub-IPCs.
INR	• Authored and negotiated approval of UN General Assembly resolutions (including those related to combating the criminal misuse of information technologies, creation of a global culture of cybersecurity, protecting critical information infrastructures, and taking stock of national efforts to protect critical information infrastructures). • Participates as subject matter experts in U.S. delegations to ASEAN meetings that focus on cyberspace policy and international security, such as terrorist exploitation of the Internet. • Represents the U.S. at the UN Group of Governmental Experts. • Leads U.S. efforts at the Organization for Security and Co-operation in Europe by sponsoring workshops and providing expertise on critical infrastructure protection, cyberterrorism, and cybersecurity. • Participates in OAS-CICTE conferences and workshops focused on cybersecurity and counterterrorism. • Participates in Meridian conference activities. • Engages in bilateral and multilateral relationships with foreign countries to address a range of cybersecurity issues. • Prepares analysis of international cybersecurity issues. • Coordinates the Department of State's representation to the ICI-IPC, including the International Sub-IPC.

Agency/component	Description of efforts
INL	• Provides leadership to U.S. delegations to the G8 Subgroup on High-Tech Crime. • Promotes greater acceptance and use of the UN Convention Against Transnational Organized Crime as an alternative means for countries to address cybercrime. • Provides leadership to cybercrime efforts within OAS-REMJA. • Participates in the International Sub-IPC.
EUR/RPM	• Develops and coordinates U.S. policy related to NATO, including consideration of NATO cyber defense policies and the planned revision of NATO's Strategic Concept.

Source: GAO analysis of Department of State data.

FCC

FCC is an independent federal agency charged with regulating interstate and international communications by radio, television, wire, satellite, and cable. The FCC is organized into seven bureaus, and, according to FCC officials, the International Bureau has primary responsibility for representing the FCC in satellite and international matters. FCC officials also stated that the agency has a role in the activities of the International Sub-IPC. FCC officials provided descriptions of their efforts, which we summarized in table 9.

Table 9: FCC's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of efforts
International Bureau	• Participates in ITU-R study group efforts as a member of U.S. delegations. • Participates in ITU-D study group efforts (domestic enforcement of laws, rules, and regulations on telecommunications by national telecommunication regulatory authorities) as a member of U.S. delegation. • Participates in OAS-CITEL meetings as a member of U.S. delegation. • Has attended a meeting of OECD's WPISP. • Provides technical expertise and guidance to other U.S. agencies participating in international efforts via the International Sub-IPC and Telecommunications Standardization Advisory Group.

Source: GAO analysis of FCC data.

USTR

USTR is the primary adviser to the President on international trade matters. It is responsible for developing and coordinating U.S. international trade policy and has the responsibility for trade negotiations with other countries. The Trade Agreements Act of 1979 gives USTR the responsibility for coordinating the development of U.S. trade policy on all standards-related activities. According to USTR officials, the USTR leads federal government policy deliberations on foreign standards-related measures through the interagency Trade Policy Staff Committee in order to prevent and resolve trade concerns arising from standards-related measures. In addition, it is to engage with other governments on

standards-related issues, as well as through multilateral organizations such as APEC and OECD. Further, according to USTR officials, it also has a role in the activities of the International Sub-IPC. USTR officials provided descriptions of their efforts, which we summarized in table 10.

Table 10: USTR's International Efforts Related to Cyberspace Security or Governance

Agency/component	Description of efforts
USTR	• Manages the implementation of the World Trade Organization (WTO) Agreement on Technical Barriers to Trade by monitoring other WTO members' technical regulations and conformity assessment procedures; also engages with other WTO members bilaterally and in the WTO to clarify and resolve issues. • Leads U.S. efforts to negotiate the Anti-Counterfeiting Trade Agreement Act, part of which would establish international standards for enforcing property rights in the digital environment. • Leads the Trade Policy Staff Committee and the Trade Policy Review Group to coordinate interagency policies related to international trade. • Participates in Meridian Conference activities. • Participate in OECD-WPISP meetings as a member of U.S. delegations. • Participates in APEC-TEL. • Engages with ISO on policy matters and serves as a voting member of the ANSI ISO Council and the ANSI International Policy Committee. • Provides technical expertise and guidance to other U.S. agencies participating in international efforts via the International Sub-IPC.

Source: GAO analysis of USTR data.

Federal Entities' Roles Vary

Federal entities' roles range from leading or being a member of a U.S. delegation to an international entity or effort, providing policy advice to other U.S. entities through the interagency process, and attending meetings. For example, DHS's CS&C hosted and led the 2009 Meridian conference that brought together more than 100 participants from 40 countries. In contrast, DHS participates at the biannual meetings of the OECD's WPISP as a member of the U.S. delegation. Figure 1 illustrates federal agencies' involvement with the key entities and efforts.

Figure 1: U.S. Government Involvement in Key Entities and Efforts Addressing Global Cyberspace Security and Governance

	Key entities and efforts																								
										ITU										OAS					
	APEC	ASEAN	Council of Europe	European Union	FIRST	G8 Subgroup on High Tech Crime	IEEE	IEC	ISO	ITU-T	ITU-D	ITU-R	ITU-GCA	ICANN	IETF	IGF	INTERPOL	Meridian	NATO	OAS-CICTE	OAS-CITEL	OAS-REMJA	OECD WPISP	United Nations
DOC/NTIA	x									x	x	x		x	x	x				x	x		x	
DOC/NIST							x	x	x	x					x										
DOD/OASD (GSA)										x	x								x						x
DOD/OASD (NII/DOD CIO)														x					x						
DOD/JCS																									x
DHS/CS&C	x				x					x	x							x	x	x	x		x		
DHS/USSS																	x			x		x			
DOJ/CCIPS	x	x	x	x	x	x					x		x	x			x					x	x	x	
DOJ/FBI														x											
DOJ/NSD																									x
DOJ/USNCB																	x								
STATE	x	x		x		x				x	x	x	x			x			x	x	x	x	x	x	x
FCC											x	x									x		x		
USTR	x								x									x						x	

Source: GAO analysis of agency-provided descriptions.

Note: X = The range of federal entities' roles include leading or being a member of a U.S. delegation to an international organization or effort to attending meetings.

The U.S. Government Faces Challenges in Addressing the Global Aspects of Cyberspace

The U.S. government faces a number of challenges that impede its ability to formulate and implement a coherent approach to addressing the global aspects of cyberspace, including (1) providing top-level leadership, (2) developing a coherent and comprehensive strategy, (3) coordinating across all relevant federal entities, (4) ensuring cyberspace-related technical standards and policies do not pose unnecessary barriers to U.S. trade, (5) participating in international cyber incident response, (6) differing legal systems and enforcing U.S. criminal and civil laws, and (7) defining international norms for cyberspace.

Providing Top-Level Leadership

Sustained top-level leadership is critical to adequately planning and executing activities that address issues of national importance. According to the President's *Cyberspace Policy Review*, the U.S.'s cybersecurity policy official is to lead specific near-term international goals and objectives, such as developing an international policy framework and strengthening and integrating the interagency processes to formulate and coordinate our international cybersecurity-related position. However, the recently appointed Cybersecurity Coordinator's authority and capacity to effectively coordinate and forge a coherent national approach to cyberspace policy are still under development.

In addition, while the International Sub-IPC has led international cyberspace-related policy analysis since March 2009, according to Department of Commerce officials, it does not drive agency actions but instead focuses on ensuring that all agencies are aware of each others' international cyber-related activities. A DOD official stated that, at least prior to the Cybersecurity Coordinator's appointment, the International Sub-IPC focused on identifying relevant organizations and policy areas that should be included in future interagency discussions.

Although the Departments of Commerce, Homeland Security, Justice, and State have served in leadership roles for the specific activities of the key entities and efforts identified, federal agencies have not provided top-level leadership for the U.S. on these issues. For example, although the Department of State is charged with leading other federal agencies in establishing global networks to share threat information, department officials stated that only the President or an executive entity such as the NSC possesses the necessary authority to direct agencies such as DHS to participate.

Until the Cybersecurity Coordinator provides top-level leadership, there is an increased risk that U.S. agencies will not formulate and coordinate U.S. international cybersecurity-related positions as envisioned in the President's *Cyberspace Policy Review*.

Developing a Coherent and Comprehensive Strategy

Our work has demonstrated the importance of comprehensive strategies that specify overarching goals, subordinate objectives, supporting activities, roles and responsibilities, and outcome-oriented performance metrics, as well as time frames to help ensure accountability and align

agency activities with the U.S.'s long-term economic, national security, and other interests.[19]

Although multiple federal entities are engaged in a variety of international efforts that impact cyberspace governance and security, the U.S. government has not documented a clear vision of how these efforts, taken together, support overarching national goals. In lieu of a comprehensive strategy, multiple agency officials cited a variety of documents that may inform agency policies and efforts, including the 2003 *National Strategy to Secure Cyberspace* and the 2009 President's *Cyberspace Policy Review*.

However, none of the documents, taken individually or collectively, provide a comprehensive strategy. For example, while the 2003 *National Strategy to Secure Cyberspace* states that the Department of State will lead other federal agencies, the strategy does not further articulate either specific supporting activities or time frames in which to accomplish this or other objectives. Similarly, according to the President's *Cyberspace Policy Review*, the cybersecurity policy official should lead specific near-term international goals and objectives; however, it does not further articulate either the specific supporting activities or time frames in which to accomplish this or other objectives. Officials from the Departments of State and Defense stated that, as called for by the President's *Cyberspace Policy Review*, an effort is currently under way to develop an international strategy for cyberspace. However, we have not seen any evidence of such activities and, thus, were unable to determine what progress, if any, has been made towards accomplishing this goal. In addition, in March 2010, we reported that the federal government lacked a formal strategy for coordinating outreach to international partners for the purposes of standards setting, law enforcement, and information-sharing.[20]

Unless agency and White House officials follow a comprehensive strategy that clearly articulates overarching goals, subordinate objectives, specific activities, performance metrics, and reasonable time frames to achieve results, the Congress and the American public will be ill-equipped to assess how, if at all, federal efforts to address the global aspects of

[19]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[20]GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: Mar. 5, 2010).

cyberspace ultimately support U.S. national security, economic, and other interests.

Coordinating across All Relevant Federal Entities

Interagency mechanisms that fully engage all key federal agencies are crucial to ensuring that agencies' efforts are coordinated, mutually reinforcing, and supportive of national goals. Federal agencies have relied upon a variety of forums to coordinate their international efforts that impact cyberspace governance and security.

However, federal agencies have not demonstrated an ability to coordinate their activities and project clear policies on a consistent basis. Multiple DOD officials stated that relationships among a small number of government officials—rather than a formal interagency mechanism—remain a primary means by which agencies avoid policy conflicts. For example, DOD officials stated that DOD has authority to establish relationships with foreign countries to share computer vulnerability data, but it is not required to notify other agencies when such relationships are developed, though officials stated that DOD does so as a courtesy. In addition, DOD and Department of State officials acknowledged that the announcement of the Secretary of Defense's decision to establish the Cyber Command was not coordinated with the Department of State, although DOD officials stated that the department had shared the purpose, intent, and mission with other agencies, including the Department of State. Nevertheless, the announcement was perceived by several foreign governments and other entities as a potentially threatening attempt by the U.S. government to militarize cyberspace, according to recognized experts.

By contrast, multiple agency officials stated that there are interagency mechanisms that have been effective at coordinating U.S. policy. USTR officials stated that interagency coordination had improved significantly since the inception of the ICI-IPC, and noted that the International Sub-IPC established a working group in late 2009, chaired by NIST and the National Security Agency, to ensure that the U.S. engages strategically in international standards forums.

However, while the International Sub-IPC was established in March 2009 and has been used to coordinate international cyberspace-related activities and analysis across federal agencies, some key federal entities only recently began participating, and the extent to which it fully engages all key federal entities is unclear. For example, officials from the FCC told us that they did not begin participating in the International Sub-IPC meetings until January 2010. The Cybersecurity Coordinator's staff added

that they are continuing to work on ways to improve engagement with all federal entities.

The global aspect of cyberspace may prevent any single mechanism from coordinating all U.S. policies that have the potential to affect cyberspace governance and security. Nevertheless, unless federal agencies institutionalize a coordination mechanism that engages all key federal entities, it is less likely that federal agencies will be aware of each other's efforts, or that their efforts, taken together, will support U.S. national interests in a coherent or consistent fashion.

Ensuring Cyberspace-Related Technical Standards and Policies Do Not Pose Unnecessary Barriers to U.S. Trade

U.S. and foreign technical standards and related policies—including those that address areas such as cybersecurity or privacy—can create incidental barriers to trade by forcing private companies to choose between exiting a market and redesigning their products to comply with the technical standards of a particular country. In this regard, some countries have attempted to mandate compliance with their indigenously developed cybersecurity standards in a manner that risks discriminating against U.S. companies.

For example, USTR reported that, in 2007, China proposed information security regulations that would have mandated testing and certification of security functions for information technology products such as routers, smart cards, and secure databases and operating systems sold commercially in China.[21] According to USTR, these regulations would have gone beyond internationally accepted practices by mandating testing and certification for products in the commercial sector, not just products for government use in national security applications. As a result, this information security policy could pose a trade barrier to foreign companies that seek to market and sell their products to China, according to industry groups, a European delegation to the WTO,[22] and as reported by the USTR. USTR officials stated that, after international concerns were voiced by U.S. officials and officials from other countries, China agreed in 2009 to limit the scope of the testing and certification requirements to products sold to the government.

[21]Office of the United States Trade Representative, *2010 Report on Technical Barriers to Trade* (Mar. 31, 2010).

[22]*China's Transitional Review Mechanism*, G/TBT/W/326 (Oct. 29, 2009).

Similarly, in 2009, USTR reported that the government of South Korea considered mandating adoption of an indigenous encryption standard as part of a large-scale government adoption of voice-over-Internet-Protocol systems. USTR officials stated that they successfully convinced the South Korean government to limit its plans to select South Korean government agencies, which would have otherwise forced U.S. equipment and software suppliers to customize their products to comply with the South Korean standard.

Mandatory standards proposed to improve the security of U.S. government systems may also have the potential to impact U.S. and foreign trade. Multiple private sector representatives stated that they believed cybersecurity standards imposed by the U.S. government, such as supply-chain security standards, risk encouraging other countries to erect cybersecurity-related trade barriers that would discriminate against U.S. companies.

Participating in International Cyber Incident Response

The 2003 *National Strategy to Secure Cyberspace* states that the United States will foster the establishment of an international network capable of receiving, assessing, and disseminating threat information globally. More recently, the President's *Cyberspace Policy Review* stated that the federal government should explore, consistent with our national interests, expansion of information-sharing about network incidents and vulnerabilities with our nation's major allies.

Although multiple federal agencies are parties to information-sharing or incident-response agreements with other countries, the federal government lacks a coherent approach toward participating in a broader international framework for responding to cyber incidents with global impact. U.S. and European government officials, members of the private sector, and subject matter experts told us that establishing an effective international framework for incident response is difficult for multiple reasons, including the national security concerns associated with sharing potentially sensitive information, the large number of independent organizations involved in incident response, and the absence of incident response capabilities within some countries.

Security concerns related to sharing sensitive information with foreign countries can hamper U.S. efforts to establish international incident response capabilities. A DOD official stated that there is disagreement, particularly within the U.S. intelligence community, as to whether the benefits of sharing cyber-threat information outweigh the risk of harm to

U.S. security interests should sensitive data be leaked to an adversary of the United States. An official from a European governmental entity also agreed that political and national security considerations associated with sharing sensitive data pose barriers to effective international cooperation.

According to the President's *Cyberspace Policy Review* and recognized experts, the sheer number of international entities engaged in incident response can also impede international coordination. For example, an official from a major U.S.-based software manufacturer stated that during a major 2009 cyber incident, the company had to work with each of the 27 member states of the European Union individually. Moreover, it has been reported that differences in data availability, consistency, reliability, and terminology among at least 54 national-level CERTs hinder efforts to identify cybersecurity trends, threats, and vulnerabilities among countries and/or regions.[23]

In addition, there is no internationally recognized organization responsible for coordinating an international response to a cyber incident. For example, although the 2003 *National Strategy to Secure Cyberspace* identifies FIRST as a potential basis for an international incident response capability, FIRST is not intended to have an operational capability and exercises no authority over the organization and operation of individual member teams. Moreover, the Global Response Center, which was established by the International Multilateral Partnership Against Cyber Threats, has not demonstrated that it possesses the capacity to provide a legitimate global information security service to benefit all participants, according to current and former officials from the Department of State and DHS, as well as members of the private sector. In addition, officials from multiple government agencies stated that a single authoritative international incident response organization would not be appropriate.

Further, according to Department of State and DHS officials, some countries still lack the technical capacity to establish national-level CERTs, which may hinder U.S. or foreign entities from being able to work with those countries as part of a coordinated response to a cyber incident. In particular, the absence of national CERTs may challenge efforts to establish a broader network to share information, according to DHS officials.

[23]Stuart Madnick, Xitong Li, Nazli Choucri, *Experiences and Challenges with Using CERT Data to Analyze International Cybersecurity* (September 2009).

The lack of an international framework for incident response has complicated efforts of U.S.-based multinational companies to respond to international cyber incidents. For example, an official from a large U.S.-based software company stated that the lack of guidance regarding U.S. prohibitions against interacting with certain countries complicated efforts to respond to the 2009 Confickr worm. In particular, the software company was unsure whether it was permitted to work directly with DNS providers located in countries the United States has labeled as state sponsors of terrorism. The global nature of cyber threats coupled with the absence of clear guidance to U.S.-based companies may undermine international efforts to mitigate cyber incidents.

Differing Legal Systems and Enforcing U.S. Criminal and Civil Laws

Several factors complicate the efforts to enforce U.S. criminal and civil law related to cyberspace, including the (1) differences among laws of nations, (2) insufficient technical capacity of judicial systems, and (3) inconsistent enforcement of existing laws.

The differences among laws of nations can impede U.S. and foreign efforts to enforce domestic criminal and civil laws related to cyberspace. For example, FBI and USSS officials stated that differences between U.S. and foreign privacy laws have hampered their efforts to acquire evidence for certain transnational cybercrime investigations.

To enforce criminal or civil cyber-related laws, law enforcement personnel and judicial officers require specialized skills and training. As we reported in 2007, the rapid evolution of technology and cybercrime techniques means that law enforcement agencies must continuously upgrade technical equipment and software tools.[24] As a result, competing national priorities may prevent other countries from acquiring the necessary technical expertise and tools to effectively investigate cybercrime. Moreover, DOJ officials told us that developing countries that lack such expertise may be less inclined to adopt legislation necessary to investigate and prosecute alleged acts of cybercrime.

Even countries possessing the requisite legislation and specialized skills and training may nevertheless not have the necessary political or public support to enforce their laws. In particular, agency officials stated that,

[24]GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

because most cybercrime victims are American citizens, some governments view cybercrime as primarily a U.S. problem and are therefore less likely to cooperate with U.S. law enforcement agencies. We identified similar issues related to investigating and prosecuting transborder cybercrime in 2007.[25]

As previously discussed, federal entities, including DOJ, DHS, and the Department of State, participate in efforts to address the inherent challenges imposed by transnational cybercrime. Without continued engagement with the international community, the United States faces increased risk that our law enforcement will be impeded in their efforts to investigate and prosecute cybercrime.

Defining International Norms for Cyberspace

The Center for Strategic and International Studies and the President's *Cyberspace Policy Review* acknowledge the importance of establishing international norms for cyberspace.[26] According to the Center for Strategic and International Studies, international norms, though not legally binding, can provide models of behavior that shape the policies and activities of countries. For example, the President's *Cyberspace Policy Review* calls for the United States to work toward an international norm for "sovereign responsibility," which could include establishing whether—and if so, how—the international community holds a country accountable for cyberattacks launched by its citizens. In addition, the President's *Cyberspace Policy Review* calls for the United States to work toward an international norm for the "use of force" in cyberspace, which could include defining the boundary between what constitutes a cyber attack and what constitutes cyber-espionage. According to the Center for Strategic and International Studies, some have stated that there are advantages to the United States not having specifically defined positions; however, others have stated that clear international norms concerning the use of force in cyberspace may be necessary to develop the ability to deter individuals or countries from launching some types of cyber attacks against U.S. interests.

[25]GAO-07-705.

[26]Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: December 2008).

Multiple federal agencies reported that they participate in efforts that may contribute to developing international norms for cyberspace. Department of State officials stated that the department is actively engaged in the development of international norms in forums such as the UN and the Organization for Security and Co-operation in Europe, but that developing norms is a complicated and long-term process. DOD officials also stated that the absence of agreed upon definitions for cyberspace-related terminology—sometimes referred to as a lexicon—can impede efforts to develop international norms. In addition, Department of State and DOD officials stated that CNCI directs the Department of State to develop policy approaches to deter cyber attacks against the United States; however, we have not seen any evidence of what progress, if any, has been made. Officials from the Department of State, DOD, DHS, and DOJ stated that these efforts have been coordinated, in part, through the International Sub-IPC.

Conclusions

The rapid integration of information and communication technologies into virtually every aspect of modern life and the increase in associated threats have outpaced efforts by the United States and the international community. Without top-level leadership, the federal government has not forged a coherent and comprehensive strategy for cyberspace security and governance policy. In addition, the interagency coordination processes, in particular the International Sub-IPC, have not entirely ensured that all relevant federal entities are engaged in global efforts or demonstrated that federal efforts, taken together, support national interests coherently and consistently. These challenges in U.S. leadership, strategy, and coordination have hampered the nation's ability to promote cyberspace-related technical standards and policies and establish global cyber incident response capabilities consistent with our national economic and national security interests. In addition, U.S. law enforcement efforts to investigate and prosecute crime have been complicated by the differing national legal systems, making it difficult to enforce U.S. criminal and civil law. Further, the United States has been unable to define cyberspace-related norms that may be necessary for guiding a U.S. response to cyber incidents. Until these challenges are addressed, the United States will be at a disadvantage in promoting its national interests in the realm of cyberspace.

Recommendations for Executive Action

We recommend that the Special Assistant to the President and Cybersecurity Coordinator, in collaboration with other federal entities and the private sector, take the following five actions to address the challenges identified:

- 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.
- Develop with the Departments of Commerce, Defense, Homeland Security, Justice, and State and other relevant federal and nonfederal entities, a comprehensive U.S. global cyberspace strategy that
  - articulates overarching goals, subordinate objectives, specific activities, performance metrics, and reasonable time frames to achieve results;
  - addresses technical standards and policies while taking into consideration U.S. trade; and
  - identifies methods for addressing the enforcement of U.S. civil and criminal law.
- Enhance the interagency coordination mechanisms, including the ICI-IPC, by ensuring relevant federal entities are engaged and that their efforts, taken together, support U.S. interests in a coherent and consistent fashion.
- Establish, with DHS, the Department of State, and other key U.S. and international governmental and nongovernmental entities, protocols for working on cyber incident response globally in a manner that is consistent with our national security interests.
- Determine, in conjunction with the Departments of Defense and State and other relevant federal entities, which, if any, cyberspace norms should be defined to support U.S. interests in cyberspace and methods for fostering such norms internationally.

Agency Comments and Our Evaluation

In oral comments on a draft of this report, the national Cybersecurity Coordinator and his staff generally concurred with our recommendations and stated that actions are already being taken to address them. They also made one point of clarification regarding the recommendation to develop

a global cyberspace strategy. From their perspective, specific items called for by the recommendation, including performance metrics and time frames to achieve results, would be a part of an implementation plan. We acknowledge that the national strategy would consist of multiple items, including an implementation plan.

Regarding our findings and conclusions, the Cybersecurity Coordinator and staff stated that our report does not fully portray their leadership efforts, their efforts to develop a strategy, and improvements they have made regarding interagency coordination. For example, they emphasized their engagement in establishing bilateral relationships with foreign countries, which are essential to developing international consensus on cybersecurity-related issues and gaining wider agreement in the international community. In addition, they stated that they continually improve the interaction, participation, and coordination performed at the Sub-IPC. They also stated that they are taking steps to improve the coordination within agencies, indicating that our example of the Department of State reorganization is one such instance. Further, these officials stated that coordination efforts have improved since 2009, but enhancements could be made. These efforts are consistent with our recommendations to improve U.S. global cybersecurity and governance and increase the likelihood that the United States will be able to promote its national interests in the realm of cyberspace. These officials also provided technical comments, which we incorporated, where appropriate.

We also provided a draft of this report to the Secretaries of Commerce, Defense, Homeland Security, and State; the Attorney General; the Chairman of the Federal Communications Commission; and the United States Trade Representative. In written comments on a draft of this report (see app. II), the Secretary of Commerce concurred with our recommendations that the national Cybersecurity Coordinator take steps to address identified challenges, including developing a comprehensive national strategy for global cyberspace and improving interagency coordination. In addition, the Secretary provided detailed technical comments that have been incorporated in the report, where appropriate. Also, in providing technical comments via e-mail, the Director of DHS's National Protection and Programs Directorate GAO-OIG Audit Liaison Office neither concurred nor nonconcurred with our recommendations; however, he stated that National Protection and Programs Directorate officials intend to work as needed with the Cybersecurity Coordinator to assist in the implementation of the recommendations. We incorporated DHS's technical comments provided by the Director, where appropriate. We also received technical comments via e-mail from additional officials at

the Departments of Commerce, Defense, Homeland Security, Justice, and State, and the United States Trade Representative. These comments were incorporated, where appropriate.

We also provided relevant sections of the draft report to officials from public, private, and not-for-profit institutions involved in this review. We received technical comments via e-mail from some, but not all, of these officials and incorporated their comments, where appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees; the Secretaries of Commerce, Defense, Homeland Security, and State; the Attorney General; the Chairman of the Federal Communications Commission; United States Trade Representative; and other interested parties. The report also will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact David Powner at (202) 512-9286, or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are listed in appendix III.

David A. Powner
Director, Information Technology Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify (1) significant entities and efforts addressing global cyberspace security and governance issues, (2) U.S. entities responsible for addressing cyberspace security and governance and the extent of their involvement at the international level, and (3) challenges to effective U.S. involvement in global cyberspace security and governance efforts.

To identify entities and efforts with significant influence on international cyberspace security and governance, we collected and analyzed documents, such as resolutions, charters, organizational charts, policies, reports, and studies, and conducted structured interviews with relevant federal, private sector, academic, and foreign officials. We also considered entities involved in multiple cross-entity cybersecurity interactions, as well as those identified by multiple officials or other organizations. We met with officials from public, not-for-profit, and academic institutions, including the American National Standards Institute, the Center for Strategic and International Studies, the European Commission, the European Network and Information Security Agency, the Forum of Incident Response and Security Teams, George Mason University, Georgia Institute of Technology, the Internet Corporation for Assigned Names and Numbers, the Organisation for Economic Cooperation and Development, and the Organization of American States (Inter-American Committee against Terrorism). In addition, we met with officials from private corporations and trade groups, including Defense Group Inc., EMC-RSA, Google, Intel, Microsoft, Symantec, and TechAmerica. We also observed the activities occurring at the 2009 Meridian Conference for government-to-government cooperation on global critical information infrastructure protection issues.

To identify responsible U.S. government entities and their related efforts, we collected, reviewed, and analyzed documents; gathered information on key initiatives through a data collection schedule; and conducted structured interviews with officials from responsible U.S. government entities. We considered factors such as whether entities were assigned responsibility for performing cyber-related activities by a federal statute, regulation, presidential directive, or other U.S. policy. These activities were performed, as appropriate, at the following entities:

- Department of Commerce: National Telecommunications and Information Administration and the National Institute of Standards and Technology.
- Department of Defense: Office of the Under Secretary of Defense for Policy, Office of the Assistant Secretary of Defense for Global Strategic

Affairs; Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer; and the Joint Chiefs of Staff (Strategic Plans and Policy) (J-5).

- Department of Homeland Security: National Protection and Programs Directorate's Office of Cyber Security and Communication and the United States Secret Service.
- Department of Justice: Computer Crime and Intellectual Property Section, Criminal Division; the Federal Bureau of Investigation; and the U.S. National Central Bureau of INTERPOL.
- Department of State: Bureau of Economic, Energy, and Business Affairs, International Communication and Information Policy; Bureau of Intelligence and Research; Bureau of International Narcotics and Law Enforcement; and the Bureau of European and Eurasian Affairs.
- Department of the Treasury.
- Federal Communications Commission.
- United States Agency for International Development.
- United States Trade Representative.

To determine challenges to effective U.S involvement, we gathered and analyzed relevant documents, such as our past reports and studies by various cybersecurity-related entities. We also solicited input regarding the challenges from private and public sector officials, including from the Center for Strategic and International Studies, George Mason University, Georgia Institute of Technology, Defense Group Inc., Google, Microsoft, Symantec, and TechAmerica. On the basis of the information received and our knowledge of the issues, we determined the major challenges impeding U.S. ability to formulate and implement foreign policy related to cyberspace governance and security.

We conducted this performance audit from June 2009 to July 2010, in the Washington, D.C., metropolitan area, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

June 17, 2010

Mr. David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Powner:

Thank you for the opportunity to comment on the draft report from the U.S. Government Accountability Office (GAO) entitled, *Cyberspace: U.S. Faces Challenges in Addressing Global Cybersecurity and Governance* (GAO-10-606).

We concur with the report's recommendation that the national Cybersecurity Coordinator should take steps to address identified challenges, including developing a comprehensive national strategy for global cyberspace and improving interagency coordination. The Department of Commerce's detailed response to the GAO draft report is attached.

We welcome further communications with GAO regarding this draft, and we look forward to receiving the final report. Please contact Rachel Kinney at (301) 975-8707 if you have any questions regarding this response.

Sincerely,

Gary Locke

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the person named above, Michael W. Gilmore, Assistant Director; Rebecca Eyler; Richard J. Hagerman; Kenneth A. Johnson; Kush Malhotra; Lee McCracken; and Justin M. Palk made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu