Congressional Research Service
Informing the legislative debate since 1914

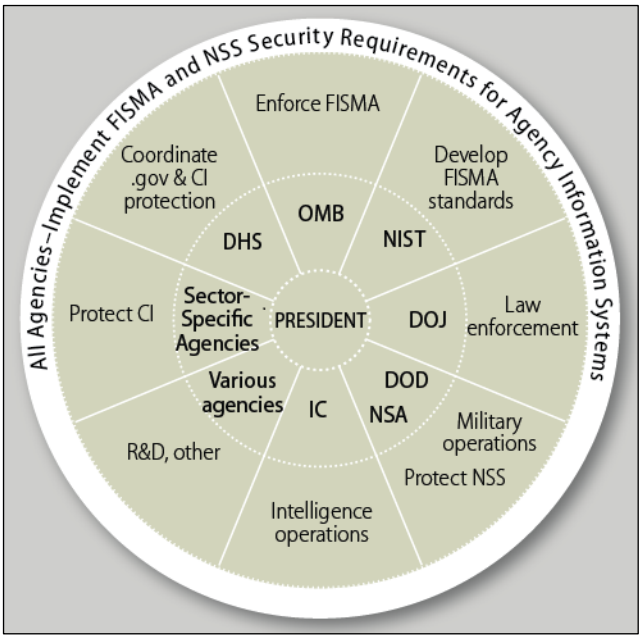
IN FOCUS

February 13, 2017

Cybersecurity: Federal Agency Roles

The federal role in cybersecurity involves both securing federal information systems and assisting in protecting nonfederal systems. All federal agencies are responsible for protecting their own systems, and many have sector-specific responsibilities for critical infrastructure (CI). A simplified overview of major roles is presented in **Figure 1** and the text below. Because of factors such as the continuing evolution of both cyberspace and agency roles, the distribution of responsibilities is more complex and ambiguous than what is presented here, with a number of unresolved issues.

Figure 1. Federal Agency Roles in Cybersecurity



Source: CRS.

Note: See text for abbreviations.

All agencies. Under the Federal Information Security Modernization Act (FISMA, 44 U.S.C. 3551 ff), each agency head must provide through the agency Chief Information Officer (CIO) for the protection of agency information systems in accordance with federal requirements, including establishment of an agency information security program.

OMB—Office of Management and Budget. In addition to its budgetary role, this White House office is responsible for approving and enforcing information security requirements under FISMA for federal systems, with two exceptions. National security systems (NSS) fall under the interagency Committee on National Security Systems. FISMA also delegates to the Secretary of Defense and the Director of National Intelligence, respectively, responsibility for systems in the Department of Defense (DOD) and the Intelligence Community (IC) agencies that are designated as crucial to their missions.

NIST—National Institute of Standards and Technology. This bureau of the Department of Commerce develops standards and guidance for federal systems that become mandatory under FISMA once approved by OMB (40 U.S.C. 11331). It also performs research relating to cybersecurity, develops voluntary guidance, works with government and private-sector entities to develop cybersecurity best practices, and coordinates interagency efforts in cybersecurity education, training, and workforce development through the National Initiative for Cybersecurity Education (NICE). The agency also coordinated the public/private development of a framework for CI cybersecurity, released in 2014.

DHS—Department of Homeland Security. FISMA provides DHS primary responsibility for coordinating the operational security of nonexcepted federal systems, including the issuing of binding operational directives for implementing FISMA requirements and of emergency directives in response to substantial threats. The Cybersecurity Act of 2015 (CSA, P.L. 114-113, div. N) also authorized and requires agencies to utilize a DHS intrusion prevention and detection program for federal civilian systems, implemented as the National Cybersecurity Protection System (NCPS) and its EINSTEIN component. The DHS Continuous Diagnostics and Mitigation (CDM) program provides tools and services to identify and mitigate vulnerabilities on agency networks.

In addition, DHS oversees federal efforts to coordinate and improve the protection of U.S. CI, most of which is controlled by the private sector. The National Cybersecurity Protection Act of 2014 (P.L. 113-282) authorized the National Cybersecurity and Communications Integration Center (NCCIC), established administratively in 2009, to provide and facilitate information sharing and incident response among public and private-sector CI entities. The CSA established a process to facilitate public- and private-sector sharing of information on cyberthreats and defensive measures through the NCCIC and other means, and it permits private-sector entities to monitor and operate defenses on their information systems.

DOJ—Department of Justice. Much of the enforcement of federal criminal laws relating to cybersecurity, including investigation and prosecution, is carried out by DOJ. However, some entities within other departments also have enforcement responsibilities, such as the U.S. Secret Service in DHS and the Defense Cyber Crime Center in DOD. The duties of law-enforcement agencies often involve digital forensics, electronic surveillance, and other technological activities. The Federal Bureau of

Investigation (FBI) leads the multiagency National Cyber Investigative Joint Task Force (NCIJTF), which focuses on information sharing and analysis for law enforcement relating to cyberthreats.

DOD—Department of Defense. DOD is responsible for military operations in cyberspace. That includes both defensive and offensive operations, with the U.S. Cyber Command serving as the main focus for coordinating and conducting such activities. DOD agencies such as the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA) also engage in cybersecurity research and development (R&D). NSA and other DOD agencies also provide assistance upon request to DHS, other civilian agencies, and private-sector entities under various agreements.

IC—Intelligence Community. The IC consists of 17 federal agencies and other entities responsible for various forms of intelligence collection, sharing, and operations, including those relating to cybersecurity. The Director of National Intelligence sets standards for mission-crucial IC systems other than NSS.

NSA—National Security Agency. While NSA is a major component of the IC, it also has a significant cybersecurity mission, serving as the designated manager of national security systems (NSS), which are information and telecommunications systems that are used in military, intelligence, and other national security activities or that handle classified information. This includes the development of security standards. NSA, along with DHS, is also involved in designation of academic centers of excellence in cybersecurity.

DOE—Department of Energy. DOE supports cybersecurity efforts in the energy sector, including electricity and nuclear, for example by assisting private-sector energy companies in developing cybersecurity capabilities for energy-delivery systems. It also provides some cybersecurity services to other agencies and private-sector entities through the DOE National Laboratories and other means. Several of DOE's 17 national laboratories also engage in cybersecurity R&D, education and training, and other activities. These include such things as modeling and simulation of systems and networks, forensic analyses, and providing test beds for investigating and improving the security of industrial control systems.

FTC—Federal Trade Commission. Under the Federal Trade Commission Act, the FTC is required to prevent the use of "unfair or deceptive acts or practices in or affecting commerce" by businesses (15 U.S.C. 45). Several other laws also provide the agency with related authorities. The FTC has investigated many cases involving the cybersecurity practices of businesses, with settlements typically requiring the implementation of comprehensive cybersecurity programs and other actions. Many of those actions involve consumer protection, but some have involved the cybersecurity practices of companies such as hotels, financial institutions, and information and communications technology businesses.

OSTP—Office of Science and Technology Policy. This White House office coordinates and facilitates interagency and multiagency cybersecurity activities, especially R&D.

NSF—National Science Foundation. This independent agency funds research and education in cybersecurity, largely through academic and nonprofit institutions. Its Scholarship-for-Service (CyberCorps) program also provides scholarships to train cybersecurity professionals.

SEC—Securities and Exchange Commission. Federal law requires publicly traded companies and other entities registered with the SEC, with certain exceptions, to report annually on the establishment and maintenance by management and the effectiveness of "an adequate internal control structure and procedures for financial reporting" (15 U.S.C. 7262). To the extent that records are kept electronically, such a structure would include cybersecurity provisions. In addition, SEC guidance states that such entities should disclose cybersecurity risks and incidents where they form significant risk factors for investment.

SSAs—Sector-Specific Agencies. SSAs are those federal agencies responsible for leading public/private collaborative efforts to protect the 16 designated CI sectors. Plans developed for each sector include discussion of cybersecurity concerns and activities.

Regulatory Agencies. The regulatory environment for cybersecurity is complex, involving both technical and nontechnical activities by various agencies. Cybersecurity in some CI sectors is subject to specific regulations, such as the chemical (DHS), bulk electric power (Federal Energy Regulatory Commission), financial services (Department of the Treasury and other agencies), and healthcare (Department of Health and Human Services) sectors. Some agencies with regulatory authority over certain sectors, such as the Federal Communications Commission (FCC), have chosen to focus on voluntary compliance.

Other Agencies. In addition to the work of NIST, the Department of Commerce is involved in Internet policy more broadly through the National Telecommunications and Information Administration (NTIA), and, along with the Department of State, in international trade and diplomatic activities relating to cybersecurity. The General Services Administration (GSA) is involved in aspects of cybersecurity involving acquisition of goods and services, including cloud computing, by federal agencies. The Government Accountability Office (GAO) investigates agency implementation of cybersecurity programs and requirements, and agency Inspectors General (IGs) audit agency conformance to FISMA and other requirements.

Issues. Among unresolved issues are the authority of CIOs, the proper role of regulation in the cybersecurity of CI, the use of OMB authority to enforce FISMA requirements, the role of DHS in FISMA enforcement and CI cybersecurity, and the role of NSA in protecting civilian systems.

Eric A. Fischer, Senior Specialist in Science and Technology

Disclaimer