Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

March 1, 2017

Cybersecurity Legislation in the 113th and 114th Congresses

The legislative framework for cybersecurity is complex, with more than 50 federal laws affecting various aspects of it. Nevertheless, since the 111th Congress, more than 300 bills have been introduced that would address a range of cybersecurity issues. Several that were enacted in the 113th and 114th Congresses are discussed below. Those bills addressed five main topics:

Protection of Federal Information Systems: updating federal agency requirements to reflect changes in technology and the threat landscape, and establishing Department of Homeland Security (DHS) authorities to protect federal systems.

Information Sharing: facilitating public- and private-sector sharing of information on cyberthreats and defensive measures and permitting private-sector entities to monitor and operate defenses on their information systems.

Statutory Authorization of Ongoing Activities:

- DHS—the National Cybersecurity and Communications Integration Center (NCCIC) and the intrusion-protection system known as EINSTEIN.
- National Institute of Standards and Technology (NIST)—relating to the Framework for Improving Critical Infrastructure (CI) Cybersecurity and the National Initiative for Cybersecurity Education (NICE).
- National Science Foundation (NSF)—the CyberCorps: Scholarship-for-Service program to train new cybersecurity professionals.

Research and Development (R&D): requiring a multiagency strategic plan for cybersecurity R&D and specifying areas of research for NSF.

Federal Cybersecurity Workforce: requiring the Office of Personnel Management (OPM) to establish and implement an employment-code structure for federal cybersecurity personnel and improving the size, skills, and preparation of the DHS cybersecurity workforce, including recruitment.

Other Provisions required the following:

- DHS to develop and exercise incident-response plans for cybersecurity risks to CI,
- DHS and NIST to assist states in improving cybersecurity for emergency response networks,
- the Department of Health and Human Services (HHS) to assist the healthcare sector in reducing cybersecurity risks,
- the Office of Management and Budget (OMB) to establish procedures for notification and other responses to federal agency data breaches of personal information,
- the Department of State to produce an international cyberspace policy and engage in international consultations on measures against cybercriminals, and
- various federal agencies to report to Congress on specified cybersecurity topics and activities.

The provisions summarized above are in the bills cited in **Table 1**.

Table 1. Cybersecurity Laws Enacted in 2014 and 2015

Public Law	Title
P.L. 113-246	Cybersecurity Workforce Assessment Act
P.L. 113-274	Cybersecurity Enhancement Act of 2014
P.L. 113-277	Border Patrol Agent Pay Reform Act of 2014
P.L. 113-282	National Cybersecurity Protection Act of 2014—NCPA
P.L. 113-283	Federal Information Security Modernization Act of 2014—FISMA 2014
P.L. 114-113	Cybersecurity Act of 2015 (Division N)—CSA
	Cybersecurity Information Sharing Act (Title I)—CISA
	National Cybersecurity Protection Advancement Act of 2015 (Subtitle A of Title II)—NCPPA
	Federal Cybersecurity Enhancement Act of 2015 (Subtitle B of Title II)—FCEA
	Federal Cybersecurity Workforce Assessment Act of 2015 (Title III)
	Other Cyber Matters (Title IV)

Source: CRS.

The **Cybersecurity Workforce Assessment Act** required an assessment by DHS of its cybersecurity workforce and development of a workforce strategy. The **Border Patrol Agent Pay Reform Act of 2014** provided additional hiring and compensation authorities to DHS and required a DHS assessment of workforce needs.

The **Cybersecurity Enhancement Act** contained the provisions on R&D and on NIST and NSF program authorizations described above.

NCPA provided statutory authority for the DHS NCCIC, and specified both public- and private-sector members. The act gave NCCIC responsibility for sharing timely and actionable cybersecurity information, providing situational awareness and coordination of information across sectors, performing integration and analysis of risks and incidents, providing technical assistance upon request, and making recommendations for improving cybersecurity.

The act also requires DHS to develop and exercise incident-response plans for cybersecurity risks to CI and to provide security clearances to appropriate representatives.

NCPA also has a provision on OMB data-breach notification policies similar to that in FISMA 2014 (see below).

FISMA 2014 updated the Federal Information Security Management Act (FISMA 2002). FISMA 2014 retains, with some amendments, most provisions of the earlier law. Notable changes include providing statutory authority to DHS for overseeing operational cybersecurity of federal civilian information systems, as well as requiring agencies to implement DHS-issued directives and to use DHS automated tools for cybersecurity protection.

It requires OMB to update periodically data-breach notification policies and guidelines for agencies, including notification of Congress and affected individuals.

The four titles of the **CSA** address information sharing, the security of federal systems, the federal cybersecurity workforce, international cybercrime and cyberspace policy, and cybersecurity in the healthcare and emergency services sectors, as well as other issues, and it includes a number of reporting requirements.

CISA (Title I) requires the Director of National Intelligence (DNI), the Secretaries of Homeland Security and Defense, and the Attorney General (AG), in consultation with federal agencies, to jointly establish procedures for sharing classified and unclassified cybersecurity information with relevant federal and nonfederal entities.

It gives private entities the authority to monitor and defend their own systems, and others where authorized, and to voluntarily share threat information and defensive measures with each other and the federal government, with protections for security, privacy, nondisclosure, and correction of errors. Covered activities are exempted from antitrust laws, and entities performing them are protected from liability. However, the act also specifies actions that are not permitted under the antitrust exemption.

As required by CISA, DHS and the Department of Justice (DOJ) issued procedures and guidelines for sharing between federal and nonfederal entities, with protection of privacy and civil liberties, and prevention of unauthorized disclosure. DHS, which the act named as the main federal portal for information sharing, established a process within the department for receiving and sharing information. Receipt of information must be through that process except for regulatory and law enforcement purposes. The President may subsequently establish an additional process if needed.

Government entities may use shared information for specified purposes relating to cybersecurity, prevention of serious personal or economic harm, and law enforcement, but not for regulatory purposes except as related to prevention or mitigation of cyberthreats. CISA supersedes nonfederal laws on authorized activities, except for law enforcement. It limits the effect of its provisions on otherwise lawful disclosures, whistleblower protections, protection of sources and methods, other law on information shared with the federal government, other information sharing relationships, contractual obligations and rights, obligations for nonfederal entities to share information with the federal government, liability for not sharing, otherwise legal disclosure in criminal prosecutions, regulatory authority except as provided in the title, and the authority of the Secretary of Defense to respond to malicious cyber-activities by foreign powers. Provisions in the title expire at the end of FY2025.

NCPAA (Title II, Subtitle A) expands NCCIC responsibilities to include CISA implementation and other information sharing responsibilities across CI sectors and internationally. It permits DHS to enter into voluntary information-sharing agreements with nonfederal entities. It also requires DHS to (1) support and develop automated information-sharing mechanisms, (2) implement direct reporting by the NCCIC to the Secretary of Homeland Security of significant risks and incidents, (3) engage in public outreach on information sharing, and (4) regularly update and exercise the annex on cybersecurity of the DHS National Response Framework. DHS may also implement ways to coordinate vulnerability disclosures. The act also specifies sharing cybersecurity information as a function of Information Sharing and Analysis Organizations (ISAOs).

FCEA (Title II, Subtitle B) provides statutory authorization for the DHS EINSTEIN program, requires agency adoption of it and implementation of additional cybersecurity measures. It also gives DHS authority, in the event of a substantial threat to federal systems, to issue emergency directives for their protection, and, in the event of an imminent threat, to use intrusion-protection capabilities. Agencies must identify sensitive and mission-critical data on their systems, make such data indecipherable to unauthorized users, assess access needs and controls, and implement identity management.

The **Federal Cybersecurity Workforce Assessment Act** (Title III) requires OPM to develop personnel codes for federal cybersecurity positions, and agencies must apply those codes as appropriate.

Other Cyber Matters (Title IV)—The Department of State produced a required comprehensive international strategy for U.S. cyberspace policy under this title. It also requires the agency to consult with countries that have cybercriminals who are not likely to be extradited to the United States, to determine what crime-fighting actions the countries have taken against such criminals. It requires DHS to establish processes to enhance cybersecurity and information sharing among state emergency responders and to develop best practices for reducing cybersecurity risks to them. HHS created a required public/private taskforce to improve cybersecurity in the healthcare sector. The title also requires HHS to collaborate with other federal and sector entities to develop guidelines for reducing risks. Another provision extended criminal penalties for fraud against a U.S. entity involving devices used to access financial accounts to such uses occurring outside U.S. territory.

Eric A. Fischer, Senior Specialist in Science and Technology

Disclaimer