



No. 21

July 26, 2012

S. 3414 – Cybersecurity Act of 2012

Noteworthy

- **Floor Situation:** S. 3414 was introduced by Senators Lieberman, Collins, Rockefeller, Feinstein, and Carper on July 19, 2012. Cloture was filed July 25, 2012, on the motion to proceed to the bill. The Majority Leader has used the Rule 14 process to place it on the Senate Calendar, bypassing all committees of jurisdiction on the matter. No committee has marked-up the bill.
- **Executive Summary:** S. 3414 endeavors to secure cybersystems associated with critical infrastructure assets, as well as establish mechanisms for information sharing between the private sector and the federal government and among private sector actors themselves. It also has provisions pertaining to cyber research and development, updating the Federal Information Security Management Act (FISMA), and strengthening the federal cybersecurity workforce.

Background/Overview

The Obama Administration Cyberspace Policy Review notes that National Security Presidential Directive 54/Homeland Security Presidential Directive 23 [defines](#) cyberspace as “the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.” [Cybersecurity](#) consists of the measures taken to prevent, detect, and respond to attacks on information systems.

As the first National Strategy to Secure Cyberspace [put](#) it, we are “a nation in cyberspace,” as it is the central nervous system controlling and connecting infrastructures throughout the country. To the military, cyberspace is an operational domain just like land, sea, air, and space. National

security officials have consistently testified that U.S. reliance upon cyberspace creates enormous vulnerabilities. Leon Panetta, when he was CIA director, [warned](#) “the next Pearl Harbor could very well be a cyberattack,” as a large-scale disruption “could paralyze this country.”

Bad actors have a range of capabilities—from sophisticated state actors, such as Russia and China, on the one hand; down to terrorists, hacker groups, and individual hackers on the other. Director of National Intelligence James Clapper has [testified](#) to Congress “China and Russia are of particular concern” and that “entities within these countries are responsible for extensive illicit intrusions into U.S. computer networks and theft of U.S. intellectual property.”

The Secretary of Homeland Security has lead federal responsibility for protecting critical infrastructure. To that end, a National Infrastructure Protection Plan has been developed, which acknowledges the vast majority of critical infrastructure assets and networks are owned and operated by the private sector. There are currently 18 critical infrastructure sectors, each of which has an assigned “sector-specific agency” and a “sector coordinating council” composed of owners and operators of critical infrastructure. Together they coordinate the development and implementation of a “sector-specific plan” to apply the framework of the National Infrastructure Protection Plan to the unique characteristics and conditions of each sector.

There already exist at least six [cyber centers](#) across the federal government. The Congressional Research Service has [identified](#) more than 50 laws on the books with provisions relevant to cybersecurity. The Cybersecurity Act of 2012, S. 3414, endeavors to secure cybersystems associated with critical infrastructure assets, as well as establish mechanisms for information sharing between the private sector and the federal government and among private sector actors themselves.

House Action

On April 26, 2012, the House passed H.R. 3523, the Cyber Intelligence Sharing and Protection Act, by a [vote](#) of 248-168. As per the bill’s title, this legislation focused extensively on information sharing. On that same day it also passed H.R. 2096, the Cybersecurity Enhancement Act, by a [vote](#) of 395-10. This bill focused primarily on federal cybersecurity research and development and strengthening the federal cybersecurity workforce.

The House also passed by voice vote two other bills related to cybersecurity around that time: 1) H.R. 3834, Advancing America’s Networking and Information Technology Research and Development Act, which also focused on cybersecurity research and development; and 2) H.R. 4257, the Federal Information Security Amendments Act of 2012, which primarily updates the Federal Information Security Management Act (FISMA).

Bill Provisions

Title I – Critical Infrastructure

Title I authorizes the National Cybersecurity Council, led by the Department of Homeland Security, to carry out a new government-managed process, in partnership with the private sector, to create a framework designed to protect the country's critical infrastructure from cyber attack. The process begins with an assessment of industries where cyber risk is the greatest. Categories of critical infrastructure are then identified based on that assessment. Performance requirements to mitigate risk, known as cybersecurity practices, are then proposed by industry sector. The council will either adopt the proposed practices or alter them as it determines necessary to address risk. The bill then provides incentives to owners of critical infrastructure to adhere to those practices under a newly created government program, the Voluntary Cybersecurity Program for Critical Infrastructure.

- Section 101 creates the National Cybersecurity Council, composed of representatives from a variety of federal agencies and led by the Department of Homeland Security.
- Section 102 directs the council to designate an agency to conduct, in consultation with a variety of entities, including owners of critical infrastructure, a top-level cyber risk assessment for all sectors of critical infrastructure to determine which sectors pose the greatest immediate risk. Then, in the order of the sectors identified to be highest priority, the council is to identify categories of critical infrastructure within each sector of critical infrastructure, and then owners of critical infrastructure within each category.
 - Categories can only be identified as critical cyber infrastructure if damage or unauthorized access could reasonably result in: 1) interruption of life-sustaining services, such as energy or water, sufficient to cause a mass casualty event or mass evacuations; 2) catastrophic economic damage to the United States; or 3) severe degradation of national security.
 - Section 102(b)(5) says that commercial items that organize or communicate information electronically cannot be identified as a category of critical cyber infrastructure. It further provides that commercial information technology products also cannot be identified as a category of critical cyber infrastructure based solely on a finding that the product is capable of being used in critical cyber infrastructure.
 - Section 102(c) requires the council to notify Congress of its identifications of critical cyber infrastructure, the designation of which shall not take effect until 60 days after the notification.
- Section 103 directs the National Cybersecurity Council to establish cybersecurity practices owners of critical infrastructure can choose to meet in protecting against cyber risks.
 - Under this section, sector coordinating councils are to propose to the council cybersecurity practices sufficient to effectively remediate or mitigate cyber risks identified under the risk assessment process in section 102. These practices are to be composed of industry standards and practices or other practices developed by the sector coordinating council.

- Section 103(b) then directs the council to review and adopt the practices submitted to it, along with any changes to these practices necessary to ensure the adequate remediation or mitigation of cyber risk.
 - Section 103(e) provides further that sector coordinating councils are to develop measures providing a reasonable and cost-effective method of meeting any cybersecurity practice.
 - Section 103(g) provides that a federal agency responsible for regulating critical infrastructure may adopt the voluntary cybersecurity practices as mandatory, and if it does not, it must submit a report to Congress explaining why it did not.
 - Section 103(g)(3) further provides these cybersecurity practices developed are to complement or otherwise improve regulations or compulsory standards pertaining to the security of critical cyber infrastructure.
- Section 104 creates a new government program, the Voluntary Cybersecurity Program for Critical Infrastructure, whereby owners of critical infrastructure can apply to be certified as meeting the promulgated cybersecurity practices and receive certain benefits in exchange.
 - The council is to certify an owner of critical cyber infrastructure if the owner either certifies himself or submits a third-party assessment verifying he has implemented measures sufficient to satisfy cybersecurity practices established under section 103.
 - Section 104(c) provides an owner being so certified may receive certain things, including, to the extent possible, “relevant real-time cyber threat information.”
 - It further provides the liability protection a certified owner may receive. In any civil action for damages directly caused by an incident related to a cyber risk identified in section 102, a certified owner shall not be liable for punitive damages if the owner is in substantial compliance with the cybersecurity practices at the time of the incident. Although it appears a cause of action for compensatory damages would still lie.
- Section 105 provides the rule of construction that nothing in this title shall be construed to prevent a federal agency responsible for regulating critical infrastructure from making mandatory the voluntary cybersecurity practices developed. It further states the bill does not provide any additional authority to existing regulators.
- Section 106 provides that certain information submitted under these procedures, such as in completing the risk assessments, shall gain the protections of Homeland Security Act section 214, such as exemption from FOIA disclosure and protection from use in a civil action.
- Section 107 directs the council to submit to Congress a report on the effectiveness of this title in reducing the risk of cyber attack to critical infrastructure.
- Section 109 provides that this act is not to preempt any state laws or requirements except as provided in the liability protection provision of section 104(c)(1) or the information protection provisions of section 106.

Title II – Protecting Government Networks

This title updates the Federal Information Security Management Act of 2002 (FISMA). It expands the authority of the Secretary of Homeland Security in this area, providing that the Secretary “shall oversee agency information security policies and practices.” This includes the duty to “issue and oversee the implementation of information security policies and directives, which shall be compulsory and binding on agencies to the extent determined appropriate by the Secretary.”

FISMA originally authorized the Secretary of Commerce to issue standards and guidelines pertaining to federal information systems, based on standards and guidelines developed by the National Institute of Standards and Technology. This bill maintains that authority, while further requiring the Secretary of Commerce to consult with the Secretary of Homeland Security in that process. DHS currently has the [primary responsibility](#) for the operational aspects of federal agency cybersecurity for federal information systems falling within FISMA, i.e., not national security systems.

DHS already runs an intrusion-detection system known as EINSTEIN, and this bill authorizes the Secretary of Homeland Security to “operate consolidated intrusion detection, prevention, or other protective capabilities and use associated countermeasures for the purpose of protecting agency information and information systems from information security threats.”

Section 204 amends Title II of the Homeland Security Act (HSA) to add a new subtitle pertaining to cybersecurity.

- It establishes within DHS a National Center for Cybersecurity and Communications, and transfers to it a variety of entities already existing within DHS. The new center will, among other things, manage federal efforts to secure the country’s information infrastructure.
- It directs the center to establish an information sharing program for cybersecurity threat and vulnerability information involving both public and private actors. It then provides that information shared may not be used by a federal entity in a regulatory enforcement action.

Title III – Research & Development

This title directs the Office of Science and Technology Policy, in coordination with DHS and other federal agencies, to build upon existing programs and plans to develop a national cybersecurity research and development plan. It then creates a new section 238 to the Homeland Security Act to direct DHS to carry out an R&D program to improve the security of information infrastructure.

Title IV – Education, Recruitment, & Workforce Development

This title establishes a variety of programs to promote awareness of cybersecurity issues, as well as develop and recruit a workforce dedicated to such issues. Of note, section 405 directs the Office

of Personnel Management to assess the readiness and capacity of the federal workforce to meet the federal government's cybersecurity needs. It goes on to require a variety of reports, such as on major cyber incidents involving government networks, prosecutions for cybercrime, and protecting the country's electrical grid.

Section 408 outlines the authorities of the National Center for Cybersecurity and Communications created in Title II of this bill to have access to information, its acquisition authorities, and its hiring and compensation authorities for recruiting and retention purposes.

Title V – Federal Acquisition Risk Management Strategy

This title directs DHS, in coordination with multiple federal agencies and private entities, to develop an acquisition risk management strategy to ensure the security of the federal information infrastructure. This includes processes directed at assessing the integrity of the supply chain while protecting the intellectual property of suppliers.

Title VI – International Cooperation

This title expresses the sense of Congress on the international aspects of cybersecurity.

Title VII – Information Sharing

- Section 701 provides explicit authority to a private entity to monitor its information systems for cyber threats and operate countermeasures on those systems to protect them. It authorizes information sharing among private entities regarding cyber threats for the purposes of protecting an information system.
- Section 703 directs DHS, in consultation with the DNI, Attorney General, and Secretary of Defense, to designate civilian entities as exchanges for sharing cybersecurity information. One of these exchanges is to be designated the lead exchange.
- Section 702 authorizes information sharing among private entities regarding cybersecurity threat indicators for the purposes of protecting an information system.
- Section 704, on the other hand, authorizes information sharing between non-federal entities and the federal government for the purposes of protecting an information system. It also authorizes non-federal entities to disclose cybersecurity threat indicators to a cybersecurity exchange. A non-federal entity receiving information from the exchange is to: 1) make reasonable efforts to safeguard it from unauthorized access; 2) comply with lawful restrictions placed on its disclosure; and 3) not use the information to gain an unfair competitive advantage.
- Shared information is exempt from FOIA and cannot be deemed a waiver of privilege. A federal cybersecurity exchange may only disclose shared information to law enforcement if the information appears to relate to a crime that has been, is being, or is about to be

committed; an imminent threat of death or serious bodily harm; or a serious threat to minors, including sexual exploitation. Further, it can be disclosed only in conformity with the policies and procedures pertaining to privacy and civil liberties protections this section further directs be developed.

- Section 704(g)(7) creates a new cause of action against the federal government for any person adversely affected by a willful violation of the information sharing provisions of the bill.
- Section 706 provides liability protections. First, it says that no cause of action shall lie in any court for the cybersecurity *monitoring* activities authorized in the bill. It does not, however, extinguish a cause of action for the taking of countermeasures based on information learned via the monitoring—meaning private entities essentially obtain liability protection under the bill for monitoring their systems but not for acting to protect their systems.
- It further provides no cause of action shall lie based on voluntary disclosure of cybersecurity threat indicator information to a cybersecurity exchange or to a critical infrastructure entity. This liability protection also applies to the sharing of such information with any other private entity under section 702 if that information is also disclosed within a reasonable time to a cybersecurity exchange; and to a cybersecurity services provider giving information to a customer of that provider.
- Section 706(b) goes on to create a good faith defense, providing that if a cause of action is not barred, a good faith reliance that this title permitted the conduct will be a complete defense against the cause of action. In addition:
 - Subsection (e) provides that no cause of action shall lie for the reasonable failure to act on shared information.
 - Subsection (f) provides that compliance with lawful restrictions on the disclosure of shared information is to be a complete defense to any action in tort or contract asserting a claim based on failure to disclose that information to a third party.
- Section 706(c) provides that no federal entity may use information shared as evidence in a regulatory enforcement action against the entity that shared the information.
- Sections 707(b) and (c) in tandem preempt inconsistent state law pertaining to cybersecurity services or use of cybersecurity information by private entities, while expressly preserving all other state laws or requirements.
- Section 707(e) states this title does not require a non-federal entity to share information with the federal government.

Administration Position

A [Statement of Administration Policy](#) “strongly supports” passage of the bill.

Cost

A CBO cost estimate was not available at the time of publication.

Possible Amendments

As of the publication of this notice, there is no unanimous consent agreement governing the processing of amendments.