Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Chris Jaikaran
Analyst in Cybersecurity Policy

Before

Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection
U.S. House of Representatives

Hearing on

"The Current State of DHS's Efforts to Secure Federal Networks"

March 28, 2017

Congressional Research Service
7-5700
www.crs.gov
<Product Code>

CRS TESTIMONY
Prepared for Congress

Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to testify on the current state of efforts by the Department of Homeland Security (DHS) to secure federal networks. My name is Chris Jaikaran and I am an Analyst in Cybersecurity Policy at the Congressional Research Service. In this role, I research and analyze cybersecurity issues and their policy implications.

My testimony today will address legislation recently passed by Congress, the roles and responsibilities assigned by those pieces of legislation, and the potential impact of that legislation on federal network security.

Legislation

During the 113th and the 114th Congresses, three pieces of legislation were enacted that changed how federal network security is managed. The testimony below briefly summarizes the effect of the legislation on federal network security without addressing other cybersecurity concerns, such as effects on the private sector.

Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2014 (FISMA) was enacted during the 113th Congress and codified the existing role the Department of Homeland Security (DHS) was already performing securing federal networks.[1] FISMA authorized DHS to assist OMB in developing and implementing agency information security programs, coordinating with agencies on cybersecurity, and providing assistance to agencies in achieving cybersecurity. The law also authorized DHS to issue binding operational directives, which are discussed later in this statement.

OMB is required to submit an annual report to Congress on the performance of agencies in implementing FISMA. The report for fiscal year 2016 was released on March 10, 2017, and like previous reports, is available to the public online. Agencies are also required report to their appropriate committees on their FISMA performance, but those reports are not made publically available.

National Cybersecurity Protection Act

The National Cybersecurity Protection Act of 2014 (NCPA), statutorily authorized the National Cybersecurity and Communications Integration Center (NCCIC) within DHS.[2] Enacted during the 113th Congress, this law established the NCCIC as the interface between the civilian federal government and non-federal entities for information sharing, risk analysis, and mitigation strategies related to

[1] P.L. 113-283.

[2] P.L. 113-282.

cybersecurity. The law also permits DHS to provide technical assistance to both federal and non-federal entities to support risk management and incident response, conditional upon the request of that entity.

Cyber Security Act of 2015

The Consolidated Appropriations Act of 2015 was the vehicle for the Cybersecurity Act of 2015. Enacted by the 114th Congress, this law contains four separate titles, the first of which is the Cybersecurity Information Sharing Act (or CISA).[3]

CISA authorized an information sharing program whereby cybersecurity threat information can be quickly, readily, and voluntarily shared among the private sector, between the private sector and the federal government, and among federal government agencies. CISA included provisions for the minimization of personally identifiable information, prohibitions on the government use of that data, protections for the private sector from antitrust concerns, and liability protections for sharing information. The law also authorized the application of defensive measures to mitigate known threats or security vulnerabilities on any network for which they own or have consent to take those measures from the network owner.

The second title is on National Cybersecurity Advancement. This part of the law provided authority for the NCCIC to manage the information sharing program authorized by Title I. Title II also provided authority to DHS to provide, with or without reimbursement, the ability to detect and block threats coming from the public Internet to agency networks. This capability is known in the cybersecurity community as intrusion detection systems and intrusion prevention systems, and as the National Cybersecurity Protection System (NCPS) or EINSTEIN (the name of the program DHS runs to deliver this capability). Title II also authorized DHS to develop and deploy tools to agencies which would continuously monitor the network activity of agencies' internal networks in order to detect risks and recommend mitigation activities. This is known as the Continuous Diagnostics and Mitigation program at DHS.

Title III, or the Federal Cybersecurity Workforce Assessment Act of 2015, requires federal agencies to identify the cybersecurity workforce roles of greatest need to the department and report to Congress on the progress of implementation.

Title IV contains miscellaneous cybersecurity requirements, including a study from DHS on the risks facing first responder networks.

Roles and Responsibilities

To take an organizational view, these laws established certain roles and responsibilities among federal entities for the security of the .gov domain. It may be helpful to think of OMB as the "strategic," DHS as the "operational," and individual agencies as the "tactical," with roles for NIST and agency Inspectors General, as well.

OMB, exercising its oversight of agency budgets, is responsible for overseeing agency adoption of cybersecurity practices and guiding agencies have a cybersecurity posture commensurate to their risk. Through their budgetary authority, OMB enforces the adoption of cybersecurity practices by directing the expenditure of funds for this purpose. OMB may also install new senior officials to oversee mismanaged cybersecurity programs, but CRS was unable to find an instance of OMB exercising that authority.[4]

[3] P.L. 114-113.

[4] 40 U.S.C. §11303.

DHS oversees agency adoption of cybersecurity programs, provides tools to protect agency networks, and coordinates government-wide efforts on federal cybersecurity.

Ultimately, however, agency heads are responsible for ensuring that risks are effectively managed in their own agencies, with cybersecurity being one such risk (financial and operational risk are among the others). In accordance with FISMA (P.L. 113-283) agency heads shall ensure the responsibility for cybersecurity is delegated to senior official, frequently a chief information security officer.[5]

NIST develops standards (i.e., the Federal Information Processing Standards) and guidance (i.e., Special Publications) to inform agencies of security practices to adopt.[6]

Inspectors General annually evaluate their agency's cybersecurity programs and provide recommendations on improving their agency's cybersecurity posture.

Policy Outcomes

Prior to the 113th Congress, cybersecurity risks were one of many risks that an agency head was responsible for managing, along with fiscal risk and operational risk. In managing cybersecurity risk, agencies had a responsibility to manage risk effectively, and through their collective risk management the security of the .gov domain was obtained. DHS, OMB, and NIST provided programs, information, tools, and guidance to assist agencies in managing that risk, to include EINSTEIN and FISMA guidance.[7] However, it was incumbent upon the agency to accept those tools and implement that guidance.

With the passage of the aforementioned laws enacted in the 113th and 114th Congress, including the Cybersecurity Act of 2014, Congress updated law to reflect that risk exists not just at the agency level, but across the entire federal government. Federal agencies face cybersecurity risks not just for the information that individual agencies possess. Agencies also face inherent cybersecurity risks because they exist as part of the federal government, regardless of the work of that particular agency.

The Congress statutorily affirmed the role of DHS in mitigating risk to all federal civilian agencies, reflecting the interdependent and inherent shared cyber risks agencies face. Rather than distribute risk mitigation across agency heads as their responsibility, DHS was granted authority to monitor cybersecurity risk for the .gov domain, provide tools to mitigate that risk, and assist agencies in doing so. With these authorities, DHS provides defense of agency networks at the transition point from the public Internet to the agency's networks with EINSTEIN, which improves network security.[8] DHS also provides advanced vulnerability management with CDM.[9] These tools are designed not only to strengthen security of agencies where they are deployed, but also to the federal enterprise by allowing DHS visibility to network activity across all federal agencies. This is intended to allow DHS to notice malicious activity at one agency and the opportunity to mitigate that activity at another agency before it becomes disruptive, a form of herd protection for civilian agencies. Additionally, by consolidating these responsibilities at DHS, DHS is arguably able to monitor risk to the .gov domain and take action to mitigate that risk, freeing up

[5] 44 U.S.C. §3554, (a) (3) (A).

[6] NIST, "FIPS Publications," website, October 16, 2015, at http://csrc.nist.gov/publications/PubsFIPS.html. And NIST, "Special Publications," website, April 8, 2016, at http://csrc.nist.gov/publications/PubsSPs.html.

[7] The e-Government Act of 2002 (P.L. 107-347) requires OMB to develop and issue guidance on implementing information technology security, and the Comprehensive National Cybersecurity Initiative (https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative) directed DHS to develop and deploy EINSTEIN to agencies.

[8] https://www.dhs.gov/einstein.

[9] https://www.dhs.gov/cdm.

agency resources to focus their risk at the agency level (i.e., the agency network, agency computers and data).

The distinction between the federal enterprise and the agency's enterprise appears to be continuing under the new Administration. The President's "Budget in Brief" requests $1.5 billion for DHS cybersecurity mission (to be split between their .gov and private sector security operations, but explicitly support a "more assertive defense of Government networks.").[10] Early indications from the Administration officials signal that the position of the Administration is to manage risks to the federal enterprise as a single entity.[11] Through this strategy, the Administration seeks to alleviate agency heads from having to further divide limited agency resources between mission operations and mission support, with the potential detriment to spending on the agency's cybersecurity. By shifting some additional cybersecurity actions from individual agencies to a single entity responsible for the security of all agencies the intent is to allow agencies to focus their resources on executing against the agency's mission.

Binding operational directives (BODs) are an example of the policy shift enacted with this group of legislation. These directives are compulsory direction to an agency from DHS to take specific action in order to protect the agency's information technology.[12] This is a unique relationship wherein one cabinet agency can direct another to take action—in this case, expend that agency's resources—for the purposes of managing risk to that agency, not risk to DHS. DHS is under no obligation to notify the public or Congress on the issuance of a BOD or its contents.

[10] OMB, "America First: A Budget Blueprint to Make America Great Again," budget report, 2017, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/2018_blueprint.pdf.

[11] Tom Bossert, "Cyber Disrupt 2017," remarks via video, March 15, 2017, at https://www.csis.org/events/cyber-disrupt-2017.

[12] 44 U.S.C. §3553.

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