Improving Critical Infrastructure Cybersecurity

April 2, 2019

Fiscal Year 2017 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director

April 2, 2019

The following report, "Improving Critical Infrastructure Cybersecurity," has been prepared by the Cybersecurity and Infrastructure Security Agency.

This document has been compiled pursuant to a directive in Senate Report 114-264, which accompanies the Fiscal Year 2017 Department of Homeland Security (DHS) Appropriations Act (P.L. 115-31).

This report highlights DHS's engagement with critical infrastructure where a cybersecurity incident reasonably could result in catastrophic regional or national effects identified pursuant to Section 9(a) of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, of February 12, 2013.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jon Tester
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact me at (202) 282-8260.

Sincerely,

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

This report highlights activities and initiatives that DHS has put forth to reduce the reasonable likelihood that a single cyber incident could result in catastrophic harm to public health or safety, economic security, or national security. Critical infrastructure entities where such an incident could occur are identified pursuant to Section 9(a) of Executive Order 13636. As such, this report will refer to these entities as Section 9 entities.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models, interdependent functions, systems in both the physical and cyber domains, and governance constructs that involve multilevel authorities, responsibilities, and regulations. Critical infrastructure owners and operators are positioned uniquely to manage risks to their individual operations and assets, and to determine effective, risk-based strategies to make them more secure and resilient. The Federal Government works closely with critical infrastructure partners to reduce barriers to information sharing and to provide technical assistance. The Federal Government also invests in capabilities that improve the ability of the United States to attribute cyber incidents.

DHS, in coordination with sector-specific agencies, supports a range of voluntary cybersecurity risk management efforts that support Section 9 entities by offering programs, sharing information, and providing technical assistance to help organizations reduce their individual risk. This report further details these ongoing efforts to increase the cybersecurity of Section 9 entities.

Improving Critical Infrastructure Cybersecurity

Table of Contents

I. Legislative Language 1
II. Report 2
A. Introduction 2
B. Planned Actions 3
C. Conclusion 6
Appendix: List of Abbreviations 7

I. Legislative Language

Senate Report 114-264, which accompanies the Fiscal Year (FY) 2017 Department of Homeland Security (DHS) Appropriations Act (P.L. 115-31), includes the following requirement:

> In a time of increasing cyber-threats, the Nation must ensure the critical infrastructure, which the Department has already identified as being at great risk in the event of a cyber-attack, is protected from causing catastrophic harm. NPPD, in coordination with other appropriate sector-specific agencies, shall identify the number and sophistication of successful intrusions of information systems essential to the operation of critical infrastructure identified pursuant to Section-9(a) of Executive Order 13636 of February 12, 2013. Furthermore, NPPD, in coordination with other sector-specific agencies, shall evaluate options for significantly reducing the likelihood that a single cyber-attack could reasonably result in catastrophic harm to public health or safety, economic security, or national security. An initial briefing outlining the strategy for this assessment shall be provided within 180 days of the date of enactment of this act with a final report due by the end of fiscal year 2017.

Section 2202(a)(2) of the Homeland Security Act, as amended by the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018 (P.L. 115-278), states that "[a]ny reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department." As such, the Senate Report's reference to the National Protection and Programs Directorate (NPPD) is deemed a reference to CISA.

II. Report

A. Introduction

The United States' critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models, interdependent functions and systems in both the physical and cyber domains, and governance constructs that involve multilevel authorities, responsibilities, and regulations. Critical infrastructure owners and operators are positioned uniquely to manage risks to their individual operations and assets, and to determine effective, risk-based strategies to make them more secure and resilient. The Federal Government works with CISA's critical infrastructure stakeholders closely to assist them with the mitigation of cybersecurity risk; ultimately critical infrastructure owners and operators are responsible for managing their individual risk. In addition, the Federal Government generally lacks visibility into cyber incidents or intrusions unless the entity reports it and collaborates with government in risk-minimizing efforts.

To enable the prioritization of Federal Government efforts to assist our Nation's most critical infrastructure entities, DHS, in conjunction with sector-specific agencies (SSA), currently identifies such entities per Section 9 of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity.* Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economy security, or national security." Section 9 entities have critical infrastructure that is typically highly reliant on cyber infrastructure, has a limited level of resiliency, or is highly dependent on other sectors. Prioritizing services to Section 9 entities is considered an effective and efficient way to mitigate national risk.

Since Executive Order 13636 first identified Section 9 entities in 2013, CISA and interagency partners have engaged with each Section 9 entity and accompanying sector to provide timely and relevant information about available government assistance, such as cybersecurity-related assessments, priority in incident response, and targeted cyber information sharing. Since 2013, many Section 9 entities have taken advantage of available Federal programs and assessments or have participated in engagement activities with the Federal Government.

This regular engagement provides CISA with additional opportunities to disseminate cybersecurity risk information and, in turn, improves the Federal Government's understanding of the systems or assets whose incapacity or disruption would result in catastrophic consequences.

The Federal Government engages Section 9 entities in multiple ways:

- Provides Federal Government resources to improve Section 9 entities' cybersecurity risk management;
- Shares threat intelligence and operational information with Section 9 entities;
- Receives feedback from Section 9 entities regarding capabilities that are most effective in managing their cybersecurity risks; and,
- Facilitates collaboration between Section 9 entities and the Federal Government.

To enhance the security and resilience of the Nation's most critical infrastructure throughout FY 2017, CISA and associated SSAs organized direct engagement sessions with Section 9 entities and additional Federal partners. During these sessions, the Federal Government received feedback on current engagement approaches; options for developing new capabilities or collaborative activities; and existing resources, policies, and legal obstacles.

Section 9 entities and Federal partners identified the following gaps:

- Insufficient coordinated interagency support to Section 9 entities;
- Insufficient access to classified information;
- Security clearance processing challenges;
- Lack of specificity in the current methodology for identifying Section 9 entities;
- Need to improve incident communication and coordination;
- Insufficient cross-sector information sharing;
- Reluctance of private-sector entities to report cybersecurity incidents to the Federal Government;
- Need for scalable technology to reduce cyber risks;
- Insufficient scenario-based modeling of significant consequences of attack or disruption; and,
- Insufficient identification and assessment of critical infrastructure systemic risks.

B. Planned Actions

To address the gaps that Section 9 entities and Federal partners identified, CISA and its interagency partners have been taking the following actions to support Section 9 entities in their cybersecurity risk management efforts.

Establish a National Risk Management Center

In July 2018, in response to demand from industry for better risk management integration with the Federal Government, DHS refocused its analysis and planning capabilities. To complement ongoing efforts to reduce barriers to information sharing and invest in new and better capabilities, CISA launched the National Risk Management Center (NRMC). The NRMC is a center for collaborative, sector-specific, and cross-sector risk management efforts between the private sector and government to protect our Nation's critical infrastructure. Currently, the NRMC is:

- Identifying, assessing, and prioritizing strategic risks to national critical functions;
- Collaborating on the development approaches to manage risks to critical functions; and,
- Coordinating integrated cross-sector risk management activities.

Establish a DHS Program Office to Strengthen Support to Section 9 Entities and Improve Coordination of Interagency Support

CISA serves as the central access point for Section 9 entities to engage with the Federal Government and to assist with interagency and cross-sector coordination. In FY 2018, CISA established a formal program office to lead coordination among relevant SSAs and interagency partners for Section 9.

Revisit Section 9 Methodology to Explore a More Functions-based Approach
Critical infrastructure protection efforts generally have focused on assets and organizations while insufficiently accounting for the underlying services and functions. A cross-sector approach that focuses on interdependencies and functions can define the risk calculus of assets better. In collaboration with private industry, the NRMC is identifying national critical functions through risk registries and dependency analyses, with a focus on lifeline functions. Through this public-private partnership, DHS is improving protective efforts to secure critical infrastructure. For example, CISA is identifying critical cyber supply-chain elements across critical infrastructure sectors, and is fostering secure and transparent critical infrastructure supply-chain options.

The NRMC is developing the first national critical functions list. Identified national critical functions will transition the United States away from a strictly entity-based list for Section 9, which will provide a more robust understanding of the Nation's complex risk posture.

Enhance Access to Classified Information
DHS serves as the central hub for sharing information, intelligence, and providing government cybersecurity assistance to Section 9 entities. DHS supports this effort by providing classified threat briefings and secure locations for private-sector personnel with security clearances. DHS also partners with the intelligence community to disseminate intelligence products and actionable data at the lowest classification level possible for broader dissemination. Additionally, DHS collaborates with the intelligence community to establish collection requirements and priorities that are useful to those who operate our Nation's critical infrastructure. DHS is working to improve the security clearance process for the private sector, and to increase the number of cleared personnel in critical infrastructure, particularly within Section 9 entities.

Improve Incident Communication and Coordination
Significant cyber incidents, particularly those that affect Section 9 entities, require unity of effort within the Federal Government and close coordination between the public and private sectors. To improve incident response coordination, DHS, in coordination with its interagency partners and the private sector, developed the National Cyber Incident Response Plan (NCIRP) to define roles and responsibilities that help to avoid confusion and duplication of effort. The NCIRP is exercised on a regular basis, with a specific emphasis on the role of interagency partners and the private sector during cyber incident response. DHS promotes awareness of the NCIRP and will continue to emphasize the importance of critical infrastructure operators informing the government of cyber incidents.

Improve Cross-sector Information Sharing with Section 9 Entities
DHS is focused on improving risk management coordination across sectors and between government and industry. Given the crosscutting nature of critical infrastructure technologies like industrial control systems and the Internet of Things, this improvement requires a cross-sector approach. For example, nation-state actors attempt to infiltrate critical infrastructure operations by targeting multiple sectors through a single incident or series of incidents across multiple sectors. CISA's incident response capability works to detect and disrupt adversary activity targeting cyber networks across all critical infrastructure sectors, connecting the cross-sector impacts.

CISA leads the Tri-Sector Working Group, which comprises representatives from the communications, energy, and finance service sectors, along with the corresponding SSAs. This Working Group is drafting a cross-sector (i.e., government and industry) playbook for implementing integrated risk management activities, improving information sharing, and providing input to the national critical functions list. DHS also prioritizes efforts to enlist participation by Section 9 entities in cross-sector information sharing programs such as the automated indicator sharing (AIS) capability, Cyber Information Sharing and Collaboration Program (CISCP), InfraGard, and the Electronic Crimes Task Forces.

CISCP enables actionable, relevant, and timely unclassified information exchange through trusted public-private relationships across all critical infrastructure sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps stakeholders to manage cybersecurity risks and enhances our collective ability to detect, prevent, mitigate, respond to, and recover from cybersecurity incidents.

The AIS capability enables the exchange of cyber threat indicators between and among the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although threat indicators also can be much more complicated). AIS is part of DHS's effort to create an ecosystem in which as soon as a company or Federal agency observes an attempted compromise, indicators are shared in real time across government and all critical infrastructure sector partners, protecting them from that particular threat. While AIS will not eliminate sophisticated cyber threats, it allows companies and Federal agencies to concentrate on them by preventing less sophisticated attacks. Since the creation of the AIS capability, more than 6.2 million unique indicators have been shared with participants.

Explore Incentives for Private-sector Entities to Exercise Due Care in Protecting Their Information and Information Systems

The Federal Government is working to identify additional options that would incentivize private-sector entities to protect their data and information systems better as well as to report cyber incidents to the Federal Government, where such legal reporting obligations do not exist already. The Federal Government is engaging directly with Section 9 entities on this work. Reporting cyber incidents to the Federal Government would improve the government's ability to help victims understand what happened. Furthermore, the Federal Government can share context and information about related incidents or malware, ensure proper investigation and preservation of evidence, and support timely response and recovery. Lastly, the Federal Government can alert other critical infrastructure stakeholders across all potentially affected sectors so that operators can take action before a catastrophic incident occurs.

Establish a Public-Private Initiative to Counter Supply Chain Vulnerabilities and Reduce Cybersecurity Vendor Risk

The information and communications technology (ICT) supply chain contains national security risks that government and industry must work together to address. CISA and critical infrastructure stakeholders in the Information Technology and Communications Sector Coordinating Councils established the ICT Supply Chain Risk Management Task Force. This Task Force develops recommendations in order to address key strategic challenges to identifying and managing risk associated with the global ICT supply chain and related third-party risk.

Explore New Technology to Reduce Cyber Risk

The advanced nature of cyber threats to critical infrastructure warrants deploying technological solutions to mitigate cybersecurity risk. The Federal Government is exploring the requirements for future technical assistance and capabilities to support Section 9 risk management activities that would improve the Federal Government's visibility into the risk posture of Section 9 entities.

C. Conclusion

Secure and resilient infrastructure is a national security imperative for the United States. The Federal Government supports critical infrastructure owners and operators in their cybersecurity risk management efforts in order to understand overall cybersecurity systemic risk. Assisting critical infrastructure entities with improving their cybersecurity risk management efforts is an important part of protecting the Nation from catastrophic incidents. While DHS supports critical infrastructure based on specific and cross-sector risk, owners and operators are ultimately responsible for both managing and mitigating risk. As a result, the Federal Government focuses on assisting individual stakeholders with their own risk management efforts, ultimately driving down national risk. Through identification of national critical functions, continued partnership activities, robust information sharing programs, and overall closer collaboration, especially during a cyber incident, DHS, in coordination with interagency partners, is focused on reducing risk to our Nation's critical infrastructure.

Appendix: List of Abbreviations

Abbreviation	Definition
AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
DHS	Department of Homeland Security
FY	Fiscal Year
ICT	Information and Communications Technology
NCIRP	National Cyber Incident Response Plan
NPPD	National Protection and Programs Directorate
NRMC	National Risk Management Center
Section 9	Entities identified pursuant to Section 9(a) of Executive Order 13636
SSA	Sector-Specific Agency