H.R. 6423, the "HOMELAND SECURITY CYBER AND PHYSICAL INFRASTRUCTURE PROTECTION ACT OF 2010"

As introduced by Reps. Thompson (D-MS), Clarke (D-NY) and, Harman (D-CA) on 10-17-10

Section-by-Section

Sec. 1. Short Title.

"Homeland Security Cyber and Physical Infrastructure Protection Act of 2010."

Sec. 2. Office of Cybersecurity and Communications and Cybersecurity Compliance Division.

Inserts Sections 221 to 224 at Subtitle C of title II of the Homeland Security Act. Below, please find descriptions of each section:

Sec. 221. Definitions.

Defines the following terms: (1) "common criteria for information technology security"; (2) "covered critical infrastructure"; (3) "cyber incident"; (4) "first-party regulatory agency"; and (5) "sector-specific agency."

Sec. 222. Office of Cybersecurity and Communications.

Creates the Office of Cybersecurity and Communications (Office) and the position of Assistant Secretary for Cybersecurity and Communications (Assistant Secretary). Locates the following entities within the Office of Cybersecurity and Communications: the United States Computer Emergency Readiness Team (US CERT), the Cybersecurity Compliance Division, and other components of the Department of Homeland Security (DHS) that oversee emergency, national communications, or cybersecurity.

Creates and funds the Cybersecurity Compliance Division and authorizes the Assistant Secretary to establish the position of Director of the Cybersecurity Compliance Division (Director). The Director has the following primary duties and responsibilities: (1) issue regulations; (2) serve as the first-party regulatory agency to enforce regulations for computer networks and assets in the critical infrastructure sectors for which the Office is the designated sector-specific agency; (3) and require first-party regulatory agencies and designated sector-specific agencies to work with the Director to develop and enforce regulations for critical infrastructure sectors; and (4) to delegate responsibilities for securing private sector networks that come under this Act to a first-party regulatory agency or an appropriate sector-specific agency.

Sec. 223. Department Responsibilities and Authorities for Securing Federal Government Networks.

Authorizes the Secretary, acting through the Assistant Secretary, to establish requirements for civilian nonmilitary and non-intelligence community Federal agencies to prevent, deter, prepare for, detect, report, attribute, mitigate, respond to, and recover from cyber attacks.

Requires the Assistant Secretary to establish and chair an interagency working group that includes the chief information officers from all Federal civilian agencies, the Director, the Assistant Secretary for Infrastructure Protection, and the White House Cybersecurity Coordinator. The Assistant Secretary shall invite representatives from military and intelligence-related agencies to join the group in as non-voting members. The group should adopt requirements by majority vote and report newly adopted requirements to the Office of Management and Budget (OMB) to be circulated in a government-wide memo.

Requires the interagency working group to develop and adopt risk-based, performance-based cyber security requirements for all civilian Federal agencies and to establish remedies for noncompliance. Also requires the group to make budgetary recommendations regarding the securing of Federal agency computer networks and to develop risk-management strategies to protect the Federal information infrastructure against cyber attack.

Authorizes the Assistant Secretary, acting through the Director, to enforce the requirements voted on by the interagency working group. The Assistant Secretary should require a certification of compliance from the head of each civilian Federal agency and may audit or inspect networks owned or operated by Federal civilian agencies. Also, the Assistant Secretary may impose the agreed-upon remedies, including penalties, to address agency non-compliance and OMB will execute the remedies.

Requires Federal entities to report any suspicious cyber incidents on their computer networks to the Director and to US CERT. US CERT will coordinate its response to a cyber incident with the reporting agency and work with the agency to identify the specific threat and to mitigate the possibility of future cyber incidents.

Sec. 224. Department Responsibilities and Authorities for Securing Private Sector Networks.

Requires the Director to consult with representatives from the public and private sectors in order to develop security requirements to protect the Nation's critical infrastructures. Security requirements must designate a sector-specific agency for each critical infrastructure sector. The designated sector-specific agency for

Information Technology is the Office of Cyber Security and Communications; the designated sector-specific agency for Communications is the National Communications System. Therefore, DHS, as the sector-specific agency, will regulate cybersecurity requirements within the information technology and communications sectors. First-party regulatory agencies and sector-specific agencies will regulate other critical infrastructure.

Authorizes the Secretary, acting through the Director, to establish and enforce risk-based, performance-based security requirements for private sector computer networks that support covered critical infrastructure. The Director shall develop security requirements to protect critical infrastructures with regard to the following risk factors: (1) threats related to data and data bases, physical infrastructures, and espionage; (2) vulnerabilities related to preparedness, target attractiveness, and deterrence capabilities; (3) the potential for death, injury, or serious adverse affects to human health and safety, and the potential for having a major impact on national security; (4) significant economic impact; and (5) risk factors that the Director considers significant.

Authorizes the Director to determine, in consultation with public- and private-sector representatives, which systems or assets constitute "covered critical infrastructure." The Director should consult with officials such as DHS's Assistant Secretary for Infrastructure Protection, DHS's Officer for Civil Rights and Civil Liberties, DHS' Under Secretary for Intelligence and Analysis, and the Director of National Intelligence. The Director should also consult with representatives from private-sector companies and the White House Cybersecurity Coordinator. Finally, the Director must notify first-party regulatory agencies, sector-specific agencies, and owners of covered critical infrastructure when the Director determines that a system should be categorizes as "covered critical infrastructure", and provide an reconsideration process for that designation.

The Director can only designate a system or an asset as "covered critical infrastructure" if that system or asset: (1) is within the prioritized list of critical infrastructure designated by DHS (See section 210E(a)(2)); (2) is a component part of the national information infrastructure or is essential to the operation of the system; or (3) would cause a national or regional catastrophe if it was destroyed. In determining which systems and assets should constitute covered critical infrastructure the Director should consider: (1) the risk factors mentioned in the second paragraph of this section; (2) known cyber incidents or cyber risks; (3) interdependencies between components of covered critical infrastructure; (4) the potential for mass casualties, economic consequences, and evacuations as well as the potential for the severe degradation of national security capabilities.

Requires the Director to ensure compliance with cybersecurity requirements. Entities that maintain covered critical infrastructures must submit a proposed cyber security plan that addresses the risk factors outline in this section and includes a timeline for addressing these risk factors to a first-party regulatory

agency or sector-specific agency. The appropriate agency will review the plan according to guidance provided by the Director and will either approve or disapprove of the plan. The reviewer must notify the submitter and the Director of its decision to approve or to disapprove of the plan. In the case of disapproval, the reviewer must give the reasons for the disapproval, suggest improvements, and provide a timetable for resubmission. An entity with a cybersecurity plan must certify that it has implemented the plan and may be subject to periodic inspections to determine if it is in compliance.

Requires all entities that own or operate covered critical infrastructure to report cyber incidents on their networks to their first-party regulatory agency, sector-specific agency, or the Director, and to US CERT. US CERT shall investigate a cyber security-related incident on a private network if the owner of the network invites US CERT to conduct such an investigation. After completing an investigation, US CERT must report the details of the incident and its recommendations regarding the incident to the Director and the first-party regulatory agency or sector-specific agency. Further, the Director may recommend SAFETY Act designation and certification for any entity that complies with the Director's cybersecurity requirements. Alternatively, the Director may recommend recision or suspicion of SAFETY ACT designation and certification during the period of noncompliance and may levy a civil penalty of no more than $10,000 a day for each instance of noncompliance.

Requires DHS's Cyber Security Compliance Division to publish a notice of proposed rulemaking for the regulations created under this section no later than six months after the enactment of this Act and to promulgate final regulations no later than one year after the date of the Act, following standard practice for notice and comment.

Sec. 3. Information Sharing.

Requires the Assistant Secretary to share relevant information regarding cybersecurity threats and vulnerabilities as well as responses to these threats and vulnerabilities with all Federal agencies and all owners and operators of covered critical infrastructure.

Sec. 4. Information Protection.

Requires the Assistant Secretary to designate information that relates to cyber security threats and that is communicated either between Federal agencies or between Federal agencies and the owners of covered critical infrastructure as sensitive security information and to handle, store, and disseminate this information accordingly.

Sec. 5. Cybersecurity Research and Development.

Instructs DHS's Under Secretary for Science and Technology to support research that aims to prevent, detect, and respond to acts of terrorism and cyber attacks. This research

should focus on developing responses to large-scale, high impact attacks. The research should also aim to develop: (1) more secure Internet protocols and architectures; (2) technologies that can detect cyber attacks and/ or intrusions; (3) improved mitigation and recovery methods; (4) research tools like test beds and data sets that will aid cybersecurity research; (5) cyber forensics and attack attribution; and (6) technologies that will facilitate the engineering of less vulnerable software.

The Under Secretary should coordinate research initiatives with the Under Secretary for National Protection and Programs, the Assistant Secretary for Cybersecurity and Communications, and DHS's Assistant Secretary for Infrastructure Protection. The Under Secretary should also coordinate research initiatives with representatives from other relevant Federal agencies like the National Science Foundation and the Department of Commerce.

Sec. 6. Cyber Workforce Recruitment, Development, and Retention.

Requires the Assistant Secretary to develop a strategic cybersecurity workforce plan that includes a description of the Department's cybersecurity mission as well as a description and analysis of the specialized workforce needed to satisfy the Federal agency's cybersecurity mission (near-, mid-, and long-term projections of workforce needs, strategic goals to address deficiencies in critical technical skills, recruitment strategies, ways to streamline the hiring process, personnel training).

Requires the Assistant Secretary to develop a cybersecurity curriculum to educate all Federal employees and contractors who are engaged in the design, development, or operation of civilian Federal agency computer networks. The curriculum may include various information that is related to: (1) role-based security awareness training; (2) recommended cybersecurity practices for working domestically and abroad; (3) unclassified counterintelligence information; and (4) responsibilities of Federal employees to comply with cybersecurity policies and procedures. The Assistant Secretary should also implement a strategy to provide Federal employees who work in cybersecurity-related areas with additional educational opportunities. The Under Secretary may appoint no more than 500 employees to carry out the requirements of the Act and may pay retention bonus to individuals who are appointed under the Act.