Section by Section

DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY AND INFORMATION SHARING

Sec. 1. Department of Homeland Security Cybersecurity Authority

Section 1(a) amends Title II of the Homeland Security Act of 2002 (HSA) (6 U.S.C. § 121 et seq.) by updating the assignment of the infrastructure protection responsibilities under the HSA from the Assistant Secretary for Infrastructure Protection to the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department. The reassignment reflects the creation of the Under Secretary position in prior amendments to the HSA and is consistent with current Department structure and organization.

Section 1(b) adds a new Subtitle E in Title II of the Homeland Security Act that includes the following:

Subtitle E – Cybersecurity Programs

Sec. 241. Short Title.

This section provides the short title of this Act as " ".

Sec. 242. Definitions.

This section defines the following terms for the purposes of the subtitle: "agency," "communication," countermeasure, critical infrastructure, critical information infrastructure, cybersecurity services, cybersecurity threat, electronic communication, electronic communication service, federal systems," "incident, information security," "information system," "governmental entity," "national security system," "private entity," "protect," and "wire communication."

Sec. 243. Enhancement of National Cybersecurity and Cyber Incident Response.

Section 243(a) directs the Secretary to engage in cybersecurity and other infrastructure protection activities under this title to support the functioning of federal systems and critical information infrastructure in the interests of national security, national economic security, and national public health and safety.

Section 243(b) directs the Secretary to carry out risk-informed approaches that: (1) improve the information security of federal systems and critical information infrastructure; (2) consider the economic competitiveness of United States industry; (3) promote the development and implementation of technical capabilities to operate in cyberspace in support of national goals; (4)

protect privacy and civil liberties; (5) promote greater research, innovation, training, education, outreach, public awareness, and investment in cybersecurity; and (6) foster the development of secondary markets and widespread adoption of cybersecurity technology by critical information infrastructure.

Section 243(c) authorizes the Secretary to conduct cybersecurity activities to protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against cybersecurity threats. Responsibilities of the Secretary include: (1) creating appropriate programs; (2) developing and conducting risk assessments of federal systems and critical information infrastructure, in consultation with the heads of other agencies and governmental and private entities that own and operate such systems and infrastructure; (3) fostering the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting federal systems and critical information infrastructure; (4) acquiring, integrating, and facilitating the adoption of new cybersecurity technologies and practices to keep pace with emerging cybersecurity threats and developments; (5) designating and maintaining a center to serve as a focal point within the federal government for cybersecurity. The cybersecurity center will: (A) facilitate information sharing among and between agencies; State, local, tribal and territorial governments; the private sector; academia; and international partners; (B) work with appropriate Federal and non-federal partners to prevent and respond to cybersecurity threats and incidents involving federal systems and critical information infrastructure; (C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information to appropriate Federal and non-federal partners; (D) integrate information from Federal Government and non-federal network operation centers to provide situational awareness of the Nation's information security posture and foster information security collaboration among system owners and operators; (E) compile and analyze information about risks and incidents that threaten federal systems and critical information infrastructure; and (F) provide incident detection, analysis, mitigation, and response information; (6) assisting in national efforts to mitigate communications and information technology supply chain vulnerabilities to enhance the security and the resiliency of federal systems and critical information infrastructure; (7) developing and leading a nationwide cybersecurity awareness and outreach effort; (8) establishing, in cooperation with the Director of the National Institute of Standards and Technology, benchmarks and guidelines for making the critical information infrastructure more secure; (9) developing a national cybersecurity incident response plan and supporting cyber incident response and restoration plans; (10) developing and conducting cybersecurity exercises and simulations; and (11) taking other necessary and appropriate lawful actions..

Section 243(d) directs the Secretary to (1) coordinate with the heads of relevant federal agencies; representatives of State, local, tribal, territorial, and foreign governments; the private sector, including owners and operators of critical information infrastructure; academia; and international organizations in carrying out this section; (2) coordinate the activities undertaken by agencies to

protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against risk of incidents involving such systems and infrastructure; and (3) ensure that activities authorized in this section are coordinated with other infrastructure protection and cybersecurity programs in DHS.

Section 243(e) ensures that the provision of certain assistance or information to one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

Section 243(f) is a savings clause for law enforcement and intelligence authorities.

Sec. 244. National Cybersecurity Protection Program.

Sec 244(a) directs the Secretary to carry out a program to protect federal systems from cybersecurity threats, which may include: (1) operating consolidated intrusion detection, prevention, or other protective capabilities; (2) conducting risk assessments of federal systems; (3) providing remote or on-site technical assistance; (4) ensuring common situational awareness across federal systems; (5) pursuant to section 249, directing agencies that own or operate a federal system to take specified action with respect to the operation of such system for the purpose of protecting that system or mitigating a cybersecurity threat; (6) discharging the responsibilities for federal information security set forth in chapter 35 of title 44, U. S. Code (as amended); and (7) testing and evaluating information security improvements within the Department.

Sec 244(b) authorizes the Secretary, notwithstanding any other provision of law, under specified conditions and when necessary in furtherance of the program authorized in subsection (a), to acquire, intercept, use, and disclose incoming, outgoing, and stored communications and other federal system traffic and to deploy countermeasures on such communications and traffic to protect federal systems from cybersecurity threats. Retention and disclosure of intercepted information will be limited, and users of federal systems must be notified of the authorized activities. The program must be implemented pursuant to policies and procedures issued by the Secretary and approved by the Attorney General. The Secretary must certify that activities carried out under this subsection are compliant with all requirements in this subsection.

Sec 244(c) authorizes agencies to permit the Secretary to implement the program under subsection (b) notwithstanding any other provision of law, for the purpose of protecting federal systems from cybersecurity threats or mitigating such threats.

Sec 244(d) limits the authorization under subsection (b) to renewable one-year periods and requires the Secretary to renew any certifications made under subsection (b) annually.

Sec 244(e) authorizes the Secretary to request and obtain the assistance of private entities that provide electronic communications or cybersecurity services in order to implement this program.

Sec 244(f) prohibits the acquisition, interception, use, or disclosure of communications and other system traffic by agencies under this section in a manner not authorized by this section.

Sec 244(g) directs the Secretary to coordinate with heads of appropriate agencies and consult with heads of all agencies responsible for federal systems to accomplish the purposes of this section.

Sec. 245. Voluntary Disclosure of Cybersecurity Information

Sec 245(a) authorizes private entities and state, local, and tribal governments that lawfully intercept, acquire, or otherwise obtain or possess any communication, record, or other information, notwithstanding any other provision of law and under specified conditions, to disclose that information to the DHS cybersecurity center designated by the Secretary under section 243(c)(5) for the purpose of protecting an information system from cybersecurity threats or mitigating such threats.

Under this subsection, federal agencies that lawfully obtain information are authorized, notwithstanding any other provision of law and under specified conditions, to share that information with individuals with cybersecurity responsibilities within that agency, the DHS cybersecurity center designated under section 243(c)(5), or a private entity that is acting as a service provider to the agency. Disclosures made under this subsection must be for the purpose of protecting an agency information system from cybersecurity threats or mitigating such threats.

Sec 245(b) permits DHS to further disclose information obtained under this section to appropriate governmental and private entities to protect information systems against cybersecurity threats, mitigate cybersecurity threats, or, with the approval of the Attorney General, to law enforcement entities when the information is evidence of a crime. Disclosure under this subsection shall be conducted in a manner consistent with policies and procedures under section 248. In addition, information disclosed under this section shall only be used or retained for the same purposes and consistent with policies and procedures under section 248.

Sec 245(c) requires that agencies ensure that when disclosing communications, records or other information to nonfederal governmental or private entities, these entities only use or retain such communications, records or other information consistent with policies and procedures under section 248 and only for the purpose of protecting information systems from cybersecurity threats, mitigating cybersecurity threats, or for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed. The Attorney General must approve any disclosures for law enforcement purposes prior to disclosure.

Sec 245(d) affirms that nothing in this section limits or prohibits otherwise lawful disclosures by a private entity to the Department or any other governmental or private entity not conducted under this section.

Sec 245(e) affirms that nothing in this section permits the unauthorized disclosure of classified information, information related to intelligence sources and methods, or information that is specifically subject to an ongoing court order precluding such disclosure.

Sec 245(f) exempts information disclosed to the Department pursuant to subsection (a) from disclosure under section 552(b)(3) of title 5, United States Code or comparable state law.

Sec 245(g) prohibits any use or disclosures of information obtained under this section in a manner not authorized by this section.

Sec. 246. Limitation on Liability and Good Faith Defense for Cybersecurity Activities.

Sec 246(a) prohibits civil or criminal cause of action in a federal or state court against any non-federal governmental or private entity for (1) a disclosure of any communication, record, or other information authorized by this subtitle; and (2) any assistance provided to the Department in accordance with the requirements of section 244(e).

Sec 246(b) establishes that a good faith determination that this subtitle permitted conduct that forms the basis of any civil or criminal action shall be a complete defense to such causes of action.

Sec. 247. Federal Preemption, Exclusivity, and Law Enforcement Activities

Sec 247(a) states that this subtitle supersedes any State or local law that regulates the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities or governmental entities to the extent such statute is inconsistent with this subtitle.

Sec 247(b) states that Section 244 shall constitute an additional exclusive means for the domestic interception of wire or electronic communications, in accordance with section 1812(b) of title 50, U. S. Code.

Sec 247(c) affirms that this subtitle does not authorize the Secretary to engage in law enforcement or intelligence activities that the Department is not otherwise authorized to conduct under existing law.

Sec. 248. Privacy and Civil Liberties, Oversight, Penalties For Misuse.

Sec 248(a) directs the Secretary to develop and periodically review, with the approval of the Attorney General and in consultation with privacy and civil liberties experts, policies and procedures governing the acquisition, interception, retention, use, and disclosure of information

obtained by DHS in connection with activities authorized in this subtitle. The policies and procedures shall minimize the impact on privacy and civil liberties; reasonably limit the acquisition, interception, retention, use and disclosure of information related to specific persons consistent with the need to carry out the responsibilities of this subtitle; include requirements to safeguard information that can be used to identify specific persons from unauthorized access or acquisition; and protect the confidentiality of disclosed information to the greatest extent practicable and informs recipients that the information may only be used for specified purposes.

Sec 248(b) directs the agencies to develop and periodically review, with the approval of the Attorney General and in consultation with privacy and civil liberties experts, policies and procedures governing the acquisition, retention, use, and disclosure of information obtained or disclosed by the agency in connection with activities authorized in this subtitle. The policies and procedures must be consistent with the requirements in 248(a).

Sec 248(c) directs the agencies to establish a program to monitor and oversee compliance with the policies and procedures issued under subsection (a) or (b) as well as promptly to notify the Attorney General of significant violations of such policies and procedures.

Sec 248(d) directs the agencies to provide to Congress the policies and procedures established in subsection (a) or (b).

Sec 248(e) requires the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Department, in consultation with the most senior privacy and civil liberties officer or officers of appropriate agencies to submit a joint, annual report to the Congress assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this subtitle.

Sec 248(f) requires the Privacy and Civil Liberties Oversight Board to submit a report to Congress and the President two years after enactment of this title providing its assessment of the privacy and civil liberties impact of the Government's activities under this subtitle and recommending improvements to or modifications of the law to address privacy and civil liberties concerns.

Sec 248(g) affirms that no communications, records, system traffic, or other information acquired or collected pursuant to this subtitle may be used, retained, or disclosed by governmental or private entities, except as authorized under this subtitle.

Sec 248(h) affirms that no otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subtitle shall lose its privileged character.

Sec 248(i) requires the agencies to develop and enforce appropriate sanctions for officers, employees or agents of the agency who conduct activities under this subtitle without authorization.

Sec 248(j) directs that any person who knowingly and willfully violates restrictions under this subtitle with respect to acquisition, interception, use, retention or disclosure of communications, records, system traffic, other information, or the related procedures established pursuant to section 248 shall be guilty of a misdemeanor and fined not more than $5,000 per incident.

Sec. 249. Required Security Action.

Sec 249(a) authorizes the Secretary to direct Federal agencies to take any lawful action with respect to the operation of its federal system for the purpose of protecting that system or mitigating a cybersecurity threat. The Secretary shall establish, in coordination with the Director of the Office of Management and Budget (OMB), procedures governing the circumstances under which such directive may issue under this section, including thresholds and other criteria; privacy and civil liberties protections; and notice to potentially affected third parties as may be applicable.

In order to take action under this section, the Secretary must specify the reasons for the required action and the duration of the directive; minimize the impact of directives under this section; and notify the Director of OMB and head of any affected agency.

Sec 249(b) authorizes the Secretary to use protective capabilities under the Secretary's control on federal systems without prior consultation with that agency for the purpose of ensuring the security of that system, if the Secretary determines there is an imminent threat to federal systems and a directive under subsection (a) is not likely to result in a timely response to the threat. The authorities under this subsection may not be delegated below the level of Assistant Secretary. The Director of OMB, head of the affected agencies, and associated Chief Information Officers, must be immediately notified of any action taken under this subsection.