Section by Section

CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE

Sec. 1. Short Title.

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

Sec. 2. Purposes.

Section 2 outlines the purposes of this Title. Generally, the purpose of this Title is to enhance the cybersecurity of infrastructures determined by the Secretary to be critical to national security, national economic security, and national public health and safety. Provisions of this Title provide for consultation on cybersecurity matters among all interested stakeholders, including sector-specific agencies with responsibility for critical infrastructure, agencies with responsibilities for regulating critical infrastructure, agencies with expertise regarding services provided by critical infrastructure, and the private sector. With significant involvement from the private sector, this Title facilitates the consultation in, and development of, best cybersecurity practices, while harmonizing the designation of entities as covered critical infrastructure with already existing infrastructure protection activities authorized by law. While the overall goal of this Title is to enhance the cyber security of critical infrastructures and protect security and vulnerability-related information, it also preserves principles of open government and supports the free flow of information. Moreover, this Title maintains a cyber environment that encourages efficiency and cost-effectiveness, innovation, and economic prosperity while also promoting safety, security, civil liberties, and privacy rights.

Sec. 3. Designation of Covered Critical Infrastructure.

Section 3(a) (Authority) authorizes the Secretary of Homeland Security (Secretary) to establish a process, through rulemaking, for designating entities as covered critical infrastructure.

Section 3(b) (Requirements) outlines the parameters for designating an entity as covered critical infrastructure. An entity may not be designated as covered critical infrastructure unless: (1) the incapacity or disruption of the reliable operation of the entity would have a debilitating effect on national security, national economic security, national public health or safety; and (2) the entity is dependent upon information infrastructure to operate. Thus, only the most critical entities would be regulated under this Title. In addition, the Secretary must consider a number of factors in order to evaluate cybersecurity risks and consequences by sector, including: interdependencies among components of covered critical infrastructure; the relative size of the entity; and the potential for destruction or disruption of the entity to cause severe, negative consequences to the nation.

Section 3(c) (Establishment of Risk-based Tiers) requires the Secretary to establish risk-based tiers within the designation process for covered critical infrastructure. Risk-based tiering recognizes that some systems, assets, or operations, for example, are more critical than others and therefore warrant greater protection. Subsection (c) requires the Secretary to assign entities into the appropriate risk-based tier based on the severity of the threat of a cyber attack, the entity's vulnerabilities to a cyber attack, the extent of consequences of a cyber attack, and such other factors as the Secretary determines to be appropriate.

Section 3(d) (Lists of Covered Critical Infrastructure) requires the Secretary to establish lists of covered critical infrastructure, which shall be periodically reviewed and updated. Inclusion on a list would be subject to judicial review under the Administrative Procedures Act (APA).

Sec. 4. Risk Mitigation for Covered Critical Infrastructure.

Section 4(a) (Cybersecurity Risks) requires the Secretary, through rulemaking, to establish a process for identifying specific cybersecurity risks that must be mitigated to ensure the security of covered critical infrastructure. The Secretary must review and designate frameworks to address such identified risks and update such risks on a regular basis. The cybersecurity risks must account for the criticality of specific systems.

Section 4(b) (Frameworks for Addressing Cybersecurity Risks) requires the Secretary to work with a wide range of interested parties (including, for example, representatives of organizations that coordinate the development of voluntary consensus standards, State and local governments, agencies, and the private sector) to propose standardized frameworks to address cybersecurity risks.

The Secretary must, in consultation with appropriate private sector representatives, consider the extent to which such proposed frameworks enhance security in practice, including criteria such as whether they reasonably address the cybersecurity risks, are cost-effective, emphasize outcome-based metrics for measuring the effectiveness of mitigating identified cybersecurity risks, and include practical evaluation focusing on performance.

The Secretary, in consultation with the appropriate agencies, must review the proposed standardized frameworks, and designate and periodically update the designation of one or more frameworks selected.

If the Secretary determines that no proposed standardized framework meets the required criteria, the Secretary must adopt a framework that meets such criteria. As part of this process, the Secretary must invite the Director of the National Institute of Standards and Technology to provide advice and guidance on possible alternative frameworks. The frameworks adopted cannot require the use of a particular measure to mitigate the risk.

Sec. 5. Cybersecurity Plans.

Section 5 requires owners or operators of covered critical infrastructure to develop cybersecurity plans that identify the measures selected by the covered critical infrastructure to address the identified cybersecurity risks. Company officers would certify that plans are being implemented, and DHS, or an agency with responsibility for regulating the entity, would have the option to review the cybersecurity plans.

Sec. 6. Evaluations.

Section 6(a) (In General) requires the Secretary, through rulemaking, to establish a process for evaluating the covered critical infrastructure's mitigation of identified risks to include: the selection of accreditors responsible for certifying evaluators to perform evaluations of covered critical infrastructure; the accreditation process for evaluators; the roles and responsibilities of evaluators in measuring the effectiveness of covered critical infrastructure in managing and mitigating cybersecurity risks; and generally-accepted evaluation practices.

Section 6(b) (Accreditation and Evaluation Process) requires the Secretary to enter into an agreement with a selected accreditor(s) with expertise in managing or implementing accreditation and evaluation programs for consensus standards. The selected accreditor(s) will conduct activities to carry out accreditations and oversee the evaluation process of covered critical infrastructure. The Secretary and the selected accreditor(s) may monitor and inspect the operations of any evaluator to ensure that the evaluator is complying with the procedures and requirements established through the rulemaking process. The Secretary and the selected accreditor(s) may revoke the accreditation of any evaluator that does not meet or comply with the established procedures and requirements, and may review any evaluation conducted by the evaluator.

Section 6(c) (Evaluations) requires covered critical infrastructure to be regularly evaluated by evaluators. The evaluations must produce outcome-based metrics that measure the effectiveness of the measures selected by the covered critical infrastructure to mitigate the identified cybersecurity risks. The evaluations must be conducted on at least an annual basis.

Sec. 7. Disclosure.

Section 7(a) (Annual Certifications) requires the Chief Executive Officer or other accountable corporate officer of a privately-held company that controls covered critical infrastructure to certify annually to the Secretary that the cybersecurity plan required by section 5 has been developed and is being implemented, the evaluation of the company's efforts to mitigate identified cybersecurity risks required by section 6 has been completed according to schedule, and whether the evaluation has concluded that the covered critical infrastructure is effectively mitigating identified cybersecurity risks.

Section 7(b) (Publicly Held Companies) requires the Chief Executive Officer or other accountable corporate officer of a company that is required to file reports under the Securities

Exchange Act and that controls covered critical infrastructure to certify annually to the Secretary that the cybersecurity plan required by section 5 has been developed and is being implemented, the evaluation of the company's efforts to mitigate identified cybersecurity risks required by section 6 has been completed according to schedule, and whether the evaluation has concluded that the covered critical infrastructure is effectively mitigating identified cybersecurity risks. It also authorizes the Securities and Exchange Commission to issue rules or regulations as necessary and appropriate to carry out the purposes of this subsection.

Section 7(c) (Public Disclosure of Cybersecurity Plans and Certifications) requires the Secretary, through rulemaking, to require owners or operators of covered critical infrastructure to publicly disclose high-level summaries of the cybersecurity plans and evaluations. Such disclosures cannot include proprietary information or other information indicating a weakness of the covered critical infrastructure.

Section 7(d) (Notification of Cybersecurity Incidents) authorizes the Secretary, through rulemaking, to require owners or operators of covered critical infrastructure to promptly report to the Secretary any significant cybersecurity incident. Subsection (c) also requires the Secretary to develop, with the approval of the Attorney General, internal reporting and dissemination procedures to notify appropriate agencies of any significant cybersecurity incidents. These internal procedures will ensure that the appropriate agency is notified of the incident and can promptly investigate it.

Section 7(e) (Protection from Public Disclosure) authorizes protection from public disclosure. For example, security and vulnerability-related information developed or collected under this Title and provided to the Federal government – including aggregated data and analysis – is exempted from disclosure under the Freedom of Information Act. Subsection (d) also authorizes a rulemaking process to prohibit the public disclosure of security and vulnerability-related information developed or collected under this Title, with exceptions provided for the sharing of information, as appropriate, to mitigate cybersecurity threats or further the official functions of a government agency, with a committee of Congress authorized to have the information, and if disclosure is required under the federal securities laws.

Section 7(f) recognizes the continued protection from unauthorized disclosure for classified information. The purpose of these provisions is to prevent the unauthorized disclosure of cybersecurity vulnerability and security information that would be used by those seeking to exploit such vulnerabilities.

Sec. 8. Enforcement.

Section 8(a) (In General) requires the Secretary, through rulemaking, to determine if the covered critical infrastructure is sufficiently addressing the identified cybersecurity risks by reviewing the cybersecurity plan developed under Section 5 and the evaluation conducted under Section 6 and

conducting periodic quality control reviews. If the Secretary determines, after conducting such a review, that covered critical infrastructure is not sufficiently addressing identified risks, the Secretary may enter into discussions, or request another agency with sector-specific expertise to enter into discussions, with the owner or operator on ways to improve the cybersecurity plan or evaluation; after having such discussions, the Secretary may issue a public statement that the covered critical infrastructure is not sufficiently addressing the risks, and take such other action as may be appropriate. Subsection (a), however, prevents the Secretary from issuing a shutdown order, requiring the use of a particular measure to address the cybersecurity risk, or imposing fines, civil penalties, or monetary liabilities. The Secretary must establish an administrative review process for covered critical infrastructure to appeal the Secretary's finding that covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks.

Section 8(b) (Special Provisions for Federal Contracts) requires the Secretary to work with the Federal Acquisition Council to amend the FAR, as necessary, in conjunction with the implementation of provisions under this Title. The purpose of this provision is to ensure that cyber security is considered in Federal contracting.

Section 8(c) (Judicial Review) establishes what is a final agency action for purposes of judicial review under the APA.

Sec. 9. Rulemaking.

Section 9(a) (In General) requires the Secretary to issue regulations under APA notice-and-comment rulemaking to carry out the provisions of this Title.

Section 9(b) (Consultation) requires that the regulations include coordination with sector-specific agencies with responsibility for critical infrastructure, agencies with responsibility for regulating critical infrastructure, and agencies with expertise regarding services provided by critical infrastructure. In addition, the regulations must include consultation with the private sector and appropriate State and local government representatives.

Section 9(c) (Exemptions) authorizes the Secretary, in coordination with OMB, to exempt covered critical infrastructure from the requirements of this Title if the Secretary determines that a sector-specific regulatory agency has sufficient specific requirements in place to effectively mitigate identified cybersecurity risks.

Sec. 10. Definitions.

This Title defines the following terms: "Agency," "Cybersecurity Threat," "Critical Infrastructure," "Incident," "Secretary," "Sector-Specific Agency," and "Selected Accreditor."