**Legislative Language**

# CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE ACT

**" SEC. 1. SHORT TITLE.**

" This Title may be cited as the "Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act."

**" SEC. 2. PURPOSE.**

" The purpose of this title is to—

" (1) enhance the cybersecurity of infrastructures determined by the Secretary to be critical to national security, national economic security, and national public health and safety;

" (2) provide for consultation on matters pertaining to cybersecurity among sector-specific agencies with responsibility for critical infrastructure, agencies with responsibilities for regulating critical infrastructure, and agencies with expertise regarding services provided by critical infrastructure;

" (3) facilitate public sector and private industry consultation and development of best cybersecurity practices by encouraging a national dialogue on cybersecurity vulnerabilities affecting critical infrastructure;

" (4) establish workable frameworks for implementing cybersecurity minimum standards and practices designed to complement, not supplant, the scope or operation of currently-available security measures;

" (5) to the maximum extent feasible and practicable, harmonize the designation of entities as covered critical infrastructure with existing infrastructure protection activities authorized pursuant to title II of the Homeland Security Act of 2002 (section 121 et seq. of title 6, United States Code);

" (6) preserve principles of open government and support the free flow of information while protecting security and vulnerability-related information; and

" (7) maintain 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.**

" (a) AUTHORITY.—Pursuant to section 9 of this title, the Secretary shall establish a process for designating entities as covered critical infrastructure.

" (b) REQUIREMENTS.—

" (1) IN GENERAL.—An entity may not be designated as covered critical infrastructure under subsection (a) unless—

" (A) the incapacity or the disruption of the reliable operation of the entity, a system or asset it operates, or a service it provides would have a debilitating impact on national security, national economic security, national public health or safety; and

" (B) the entity, a system or asset it operates, or a service it provides is dependent upon information infrastructure to operate, or is a part of information infrastructure and critical to its operation.

" (2) FACTORS TO BE CONSIDERED.—In designating entities under this section, the Secretary shall consider, but not be limited to, the following factors in order to evaluate the cybersecurity risks and consequences by sector—

" (A) interdependencies among components of covered critical infrastructure (as designated under this section);

" (B) the relative size of the entity in question; and

" (C) the potential for the incapacity or disruption of the entity, a system or asset it operates, or a service it provides to cause severe, negative consequences to national security, national economic security, and national public health and safety.

" (c) ESTABLISHMENT OF RISK-BASED TIERS.—In establishing a process for designating covered critical infrastructure, the Secretary shall establish risk-based tiers, and shall assign entities to the appropriate tier, with regard to the entity, a system or asset it operates, or a service it provides based on the severity of—

" (1) the threat of a cyber attack;

" (2) its vulnerability to a cyber attack;

" (3) the extent of consequences as a result of a cyber attack; and

" (4) such other factors as the Secretary determines to be appropriate.

" (d) LIST OF COVERED CRITICAL INFRASTRUCTURE.—The Secretary shall establish lists of covered critical infrastructure and shall periodically review and update such lists. Inclusion on a list of covered critical infrastructure shall be considered a final action for purposes of judicial review in accordance with section 702 of title 5, United States Code.

**" SEC. 4. RISK MITIGATION FOR COVERED CRITICAL INFRASTRUCTURE.**

" (a) CYBERSECURITY RISKS.—

" (1) Pursuant to section 9 of this title, the Secretary shall establish a process to--

" (A) identify specific cybersecurity risks that must be mitigated to ensure the security of covered critical infrastructure; and

" (B) review and designate frameworks to address such risks.

" (2) The cybersecurity risks that must be mitigated may vary by sector and tier and may take into account the criticality of specific systems, assets, functions, or services and the impact of cybersecurity risks on such specific systems, assets, functions, or services.

" (3) The Secretary shall regularly update the identified cybersecurity risks.

" (b) FRAMEWORKS FOR ADDRESSING CYBERSECURITY RISKS.—

" (1) The Secretary shall request that representatives of organizations that coordinate or facilitate the development and use of voluntary consensus standards, representatives of appropriate voluntary consensus standards development organizations, appropriate representatives of State and local governments, agencies, and the private sector, including sector coordinating councils and information sharing and analysis centers, propose standardized frameworks for addressing cybersecurity risks.

" (2) The Secretary shall, in consultation with appropriate private sector representatives, consider the extent to which the proposed frameworks enhance security in practice, including whether they—

" (A) reasonably address identified cybersecurity risks;

" (B) are cost-effective, including by prioritizing efforts toward critical systems, assets, functions, services, and actual risk, and minimizing the potential for burdens on or costs to efficiency, innovation, and economic prosperity;

" (C) emphasize outcome-based metrics for measuring the practical effectiveness of mitigating identified cybersecurity risks and are not based solely on compliance in implementation of measures or controls; and

" (D) include practical evaluation focusing on performance, including testing for vulnerabilities and simulated threats and other tests that mimic real-time system performance under attack and stress.

" (3) The Secretary, in consultation with the appropriate agencies, shall review the standardized frameworks proposed under paragraph (1) and, as appropriate, using the criteria identified in paragraph (2), designate and periodically update the designation of one or more frameworks that satisfy those criteria taking into account that the frameworks may be tailored to address the unique nature of various sectors.

" (4) If the Secretary determines that no standardized framework proposed under paragraph (1) meets the criteria in paragraph (2), the Secretary shall adopt a framework that meets the criteria set forth in paragraph (2). As part of such a process, the Secretary shall invite the Director of the National Institute of

Standards and Technology to provide advice and guidance on any possible alternative framework or frameworks in consultation with appropriate public and private stakeholders.

" (5) Frameworks shall not require the use of a particular measure, but shall leave the choice of particular measures to an entity to which the framework applies.

**" SEC. 5. CYBERSECURITY PLANS.**

" The owners or operators of covered critical infrastructure shall develop cybersecurity plans that identify the measures selected by the covered critical infrastructure to address the cybersecurity risks in a manner that complies with the regulations promulgated, and are guided by an applicable framework designated, under section 4. The cybersecurity plans shall--

" (1) be signed and attested to by an accountable corporate officer of the owner or operator of the covered critical infrastructure;

" (2) remain on file at the headquarters or primary operating location of the covered critical infrastructure; and

" (3) be available for review, inspection, and evaluation by an evaluator pursuant to section 6, the Secretary, or an agency with responsibility for regulating the entity.

**" SEC. 6. EVALUATIONS.**

" (a) IN GENERAL.—Pursuant to section 9 of this title, the Secretary shall establish a process to provide for, and develop requirements relating to—

" (1) the selection of accreditors;

" (2) the accreditation process for evaluators;

" (3) the roles and responsibilities of evaluators in measuring the effectiveness of owners or operators of covered critical infrastructure in managing and mitigating cybersecurity risks; and

" (4) generally-accepted evaluation practices.

" (b) ACCREDITATION AND EVALUATION PROCESSES.—

" (1) AGREEMENT.—The Secretary shall enter into one or more agreements with selected accreditors to carry out accreditations and oversee the evaluation process established under this section.

" (2) SELECTED ACCREDITOR PROCESS FOR ACCREDITING EVALUATORS.—To accredit evaluators under this section, selected accreditors entering into an agreement with the Secretary under paragraph (1) shall conduct

such activities as the Secretary determines to be necessary to effectively carry out accreditations of evaluators and oversee the evaluation process.

" (3) SELECTED ACCREDITOR PROCESS FOR MONITORING EVALUATIONS.—The Secretary and any selected accreditor may monitor and inspect the operations of any evaluator under this section to ensure that the evaluator is complying with the procedures and requirements established under subsection (a), and all other applicable requirements.

" (4) SELECTED ACCREDITOR PROCESS FOR REVOKING ACCREDITATIONS OF EVALUATORS.—If the Secretary or any selected accreditor determines that an evaluator is not meeting the procedures or requirements established under subsection (a), the selected accreditor shall—

" (A) revoke the accreditation of the evaluator to conduct evaluations under this subsection; and

" (B) review any evaluation conducted by the evaluator and report to the Secretary on the findings of the review, as necessary and appropriate.

" (c) ROLES AND RESPONSIBILITIES OF EVALUATORS.—Covered critical infrastructure shall be evaluated by evaluators on a schedule determined by the Secretary. Such evaluations shall produce outcome-based metrics that measure the practical effectiveness of the measures selected by covered critical infrastructure under section 5 in mitigating the identified cybersecurity risks. Such evaluations shall be updated at least on an annual basis.

**" SEC. 7. DISCLOSURE.**

" (a) ANNUAL CERTIFICATIONS.—Pursuant to section 9 of this Title, the Secretary shall require the Chief Executive Officer or other accountable corporate officer of an entity designated as covered critical infrastructure and not subject to subsection (b) to certify annually to the Secretary—

" (1) that the cybersecurity plan required by section 5 has been developed and is being implemented in an expeditious manner;

" (2) that the evaluation required by section 6 has been completed according to the schedule set forth in such section; and

" (3) whether the evaluation required by section 6 has concluded that the covered critical infrastructure is effectively mitigating identified cybersecurity risks.

" (b) PUBLICLY HELD COMPANIES.—The Securities and Exchange Commission shall require the Chief Executive Officer or other accountable corporate officer of a company that is required to file reports under sections 13(a) or 15(d) of the Securities Exchange Act and that is designated as, or owns an entity designated as, covered critical infrastructure to certify each of the requirements of paragraphs (a)(1)-(3) annually in a furnished exhibit to an Exchange Act report. The Securities and Exchange Commission

is authorized to issue such rules or regulations as are necessary or appropriate to carry out the purposes of this subsection.

" (c) PUBLIC DISCLOSURE OF CYBERSECURITY PLANS AND CERTIFICATIONS.—Pursuant to section 9 of this Title, the Secretary shall require owners or operators of covered critical infrastructure to publicly disclose high-level summaries of the cybersecurity plans required by section 5 and the evaluations required by section 6 in a manner and form determined by the Secretary. Such disclosures shall not include proprietary information or other information indicating a critical weakness of the covered critical infrastructure.

" (d) NOTIFICATION OF CYBERSECURITY INCIDENTS.—

> " (1) IN GENERAL.—Pursuant to section 9 of this title, the Secretary shall require owners or operators of covered critical infrastructure to promptly report to the Secretary any significant cybersecurity incident.
>
> " (2) NOTIFICATION TO APPROPRIATE AGENCIES.—The Secretary shall develop, with the approval of the Attorney General, internal reporting and dissemination procedures to notify appropriate agencies of any significant cybersecurity incident reported to the Secretary under paragraph (1).

" (e) PROTECTION FROM PUBLIC DISCLOSURE.—Except as otherwise provided in this title—

> " (1) security and vulnerability-related information developed or collected under this title and provided to the Federal government, including aggregated analysis and data, shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and
>
> " (2) pursuant to section 9 of this title, security and vulnerability-related information developed or collected under this title and provided to the Federal government, including aggregated analysis and data, shall be protected from public disclosure, except that this paragraph—
>
> > " (A) does not prohibit the sharing of such information, as the Secretary determines to be appropriate in order to mitigate cybersecurity threats or further the official functions of a government agency;
> >
> > " (B) does not authorize such information to be withheld from a committee of Congress authorized to request the information; and
> >
> > " (C) does not authorize such information to be withheld if disclosure is required under federal securities laws.

" (f) PROTECTION OF CLASSIFIED INFORMATION.—Nothing in this section permits the unauthorized disclosure of information that has been determined by the United States Government pursuant to an Executive order or statute to require protection

against unauthorized disclosure for reasons of national defense or foreign relations; any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954; information related to intelligence sources and methods; or activities; or information that is specifically subject to a court order or a certification, directive, or other authorization by the Attorney General precluding such disclosure.

**“ SEC. 8. ENFORCEMENT.**

“ (a) IN GENERAL.—Pursuant to section 9 of this title—

“ (1) the Secretary may conduct a review to determine if the covered critical infrastructure is sufficiently addressing the identified cybersecurity risks, including by reviewing the cybersecurity plan required by section 5 and the evaluation required by section 6, and by conducting periodic quality control evaluations. If the Secretary determines, after conducting such a review, that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks, the Secretary may—

“ (A) enter into discussions, or request another agency with sector-specific expertise to enter into discussions, with the owner or operator of the covered critical infrastructure on ways to improve the cybersecurity plan or the evaluation, which may include the provision of technical assistance;

“ (B) after discussions permitted in subparagraph (A), issue a public statement that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks; and

“ (C) take such other action as may be determined appropriate by the Secretary;

except that the Secretary shall not, in enforcing the provisions of this title, issue a shutdown order, require use of a particular measure, or impose fines, civil penalties, or monetary liabilities on the owner or operator of the covered critical infrastructure as a result of such review; and

“ (2) the Secretary shall establish an administrative review process for covered critical infrastructure to appeal a finding under this subsection that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks.

“ (b) SPECIAL PROVISIONS FOR FEDERAL CONTRACTS.—The Secretary shall work with the Federal Acquisition Regulatory Council established under section 1302 of title 41, United States Code, to amend the Federal Acquisition Regulation, as may be necessary and appropriate, in conjunction with the implementation of provisions under this title.

" (c) JUDICIAL REVIEW.—Any action pursuant subsections (a)(1)(B) or (C) shall be considered a final action for purposes of judicial review in accordance with section 702 of title 5, United States Code.

**" SEC. 9. RULEMAKING.**

" (a) IN GENERAL.—The Secretary shall promulgate regulations pursuant to section 553 of title 5, United States Code, to carry out the provisions of this title.

" (b) CONSULTATION.—Regulations promulgated under this section shall include—

" (1) coordinating with, and obtaining information from, the head of any—

" (A) sector-specific agency with responsibility for critical infrastructure;

" (B) agency with responsibilities for regulating the critical infrastructure; and

" (C) agency with expertise regarding services provided by critical infrastructure; and

" (2) consulting with, and obtaining information from, the private sector and appropriate representatives of State and local governments.

" (c) EXEMPTION.—The Secretary, in consultation with the Director of the Office of Management and Budget, may exempt in appropriate part 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.**

" In this title—

" (1) AGENCY.–The term "agency" has the meaning given that term in section 3502(1) of title 44, United States Code, as amended.

" (2) CYBERSECURITY THREAT.—The term "cybersecurity threat" means any action that may result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system.

" (3) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016 of Public Law 107-56 (section 5195c(e) of title

42, United States Code).

“ (4) INCIDENT.—The term “incident” has the meaning given that term in Chapter 35 of title 44, United States Code, as amended.

“ (5) SECRETARY.—The term “Secretary” means the Secretary of Homeland Security.

“ (6) SECTOR SPECIFIC AGENCY.—The term “sector-specific agency” means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.

“ (7) SELECTED ACCREDITOR.—The term “selected accreditor” means a nongovernment entity or entities with expertise in managing or implementing accreditation and evaluation programs for consensus standards, or a similarly qualified private sector entity, to carry out accreditations and oversee the evaluation process established under section 6 of this title.