TITLE XX: [PROTECTING CRITICAL INFRASTRUCTURE]

Sec. 00 Definitions & Responsibilities.

(a) Definitions.–

(1) Owner.–For the purposes of this title, the term “owner” shall mean the entity that owns the designated covered critical infrastructure and shall not be construed to mean a company contracted by the owner to manage, run, or operate a designated system or asset, or to provide a specific information technology product or service that is used or incorporated into a designated system or asset.

(2) Operator.–For the purposes of this title, the term "operator" shall mean an entity that manages, runs, or operates, in whole or in part, the day-to-day operations of a designated system or asset. An operator can, but does not have to be, the owner of the system or asset.

(b) Responsibility of Owner.–It shall be the responsibility of the owner of a system or asset designated as covered critical infrastructure pursuant to comply with the requirements of this Act.

Sec. 1. Sector-by-Sector Cyber Risk Assessments

The Secretary of Homeland Security, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership and Advisory Committee, and the National Cybersecurity Advisory Council, and in coordination with the Intelligence Community, the Department of Defense, the Department of Commerce, sector-specific agencies and other Federal agencies with responsibilities for regulating owners and operators of critical infrastructure shall –

(a) within 90 days of the effective date of this Act, conduct a top-level assessment of the cybersecurity threats, vulnerabilities, risks, and probability of a catastrophic incident across all

critical infrastructure sectors to determine which sectors pose the greatest immediate risk, in order to guide the allocation of resources for the implementation of this Act;

(b) beginning with the highest priority sectors identified under subsection (a), conduct, on an ongoing, sector-by-sector basis, cyber risk assessments of the critical infrastructure in a manner that –

(1) utilizes state-of-the art threat modeling, simulation, and analysis techniques;

(2) incorporates, as appropriate, any existing similar risk assessments; and

(3) considers the following factors:

(A) the actual or assessed threat, including a consideration of adversary capabilities and intent, intrusion techniques, preparedness, target attractiveness, and deterrence capabilities;

(B) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by damage or unauthorized access to critical infrastructure;

(C) the threat to or impact on national security caused by damage or unauthorized access to critical infrastructure;

(D) the extent to which damage or unauthorized access to critical infrastructure will disrupt the reliable operation of other critical infrastructure;

(E) the harm to the economy that would result from damage or unauthorized access to critical infrastructure;

(F) the risk of national or regional catastrophic damage within the United States caused damage or unauthorized access to information infrastructure located outside the United States;

(G) the overall preparedness and resilience of each sector against cyber attack, including the effectiveness of market forces at driving security innovation and secure practices; and

(H) other risk-based security factors appropriate and necessary to protect public health and safety, critical infrastructure, or national and economic security.

(b) The Secretary shall establish a process under which the owners and operators of critical infrastructure and other relevant private sector experts provide input into the risk assessments conducted under this subsection, and shall seek and incorporate private sector expertise available through established public-private partnerships, including the Critical Infrastructure Partnership and Advisory Committee and information sharing and analysis organizations. Any information submitted as part of this process shall be protected under Section 7.

(c) The Secretary and the Director of the National Institute of Standards and Technology, in consultation with owners and operators of critical infrastructure and relevant private sector and academic experts, shall develop repeatable, qualitative and quantitative methodologies for assessing information security risk, or utilize existing methodologies, and make those methodologies publicly available.

(d) Risk assessments under this section shall be submitted to the President, appropriate Federal

agencies, and the appropriate congressional committees and may be provided in a classified or unclassified form, as necessary.

Sec. 2. Procedure for Designation of Covered Critical Infrastructure

(a) Responsibility for Designation of Covered Critical Infrastructure.—

(1) In General.— The Secretary, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership and Advisory Committee, the National Cybersecurity Advisory Council and other appropriate representatives of State and local governments, shall establish a procedure for the designation of covered critical infrastructure, on a sector-by-sector basis, for the purposes of this subtitle.

(2) Duties.–In establishing this procedure, the Secretary shall –

(A) prioritize the Department's efforts based on the prioritization established under subsection (1)(a);

(B) incorporate to the extent practicable the input of owners and operators of critical infrastructure, the Critical Infrastructure Partnership and Advisory Committee , the National Cybersecurity Advisory Council and other appropriate representatives of State and local governments;

(B) coordinate with the head of the sector-specific agency with responsibility for critical infrastructure and the head of any Federal agency with responsibilities for regulating the critical infrastructure;

(C) develop a mechanism for owners of covered critical infrastructure to submit information to assist the Secretary's determinations under this section; and

(D) periodically review and update designations under this section, but no less than annually.

(b) Designation of Covered Critical Infrastructure.—

(1) Guidelines for Designation.—In designating covered critical infrastructure for the purposes of this subtitle, the Secretary shall:

(A) designate covered critical infrastructure on a sector-by-sector basis and at the system or asset level;

(B) inform owners of covered critical infrastructure of the criteria used to identify covered critical systems or assets;

(C) only designate a system or asset as covered critical infrastructure if damage or unauthorized access to that system or asset could result in –

(i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause –

(aa) a mass casualty event comparable to the consequences of a weapon of mass destruction; or

(bb) mass evacuations of a major population center or a large geographic area in the United States;

(ii) catastrophic economic damage to the United States including:

(aa) failure or substantial disruption of a United States financial market;

(bb) incapacitation or sustained disruption of a financial system; or

(cc) other systemic, long-term damage to the United States economy.

(iii) severe degradation of national security or national security capabilities, including intelligence and defense functions.

(D) consider the sector-by-sector risk assessments developed pursuant to Section 1.

(2) Limitations.— The designation of critical infrastructure is further limited as follows—

(i) A system or asset may not be designated as covered critical infrastructure under this section based solely on activities protected by the first amendment to the United States Constitution.

(ii) The following commercial items shall not be designated as covered critical infrastructure:

(a) a commercial information technology product, including hardware and software; and
(b) any service provided in support of a product specified in subparagraph (a), including installation services, maintenance services, repair services, training services, and any other services provided in support of the product.

(3) Notification of identification of system or asset.—The Secretary shall notify the owner of any system or asset designated as covered critical infrastructure no later than 30 days after such designation.

(4) Self-designation of system or asset as covered critical infrastructure. —The owner of a system or asset may request that a system or asset be designated as covered critical infrastructure if the owner determines that it meets the criteria for designation.

(5) System or asset no longer covered critical infrastructure.—

(i) If the Secretary determines that any system or asset that was designated as covered critical infrastructure no longer constitutes covered critical infrastructure, the Secretary shall promptly notify the owner of that system or asset of that determination.

(ii) If an owner determines that an asset previously self-identified as covered critical infrastructure no longer meets the criteria for designation as such, the owner shall notify the Secretary of this determination and submit to the redress process under this subsection.

(6) Definitions.–For the purposes of this subsection, the term “damage” shall have the same meaning given under 18 U.S.C. Section 1030.

(c) Redress.—

(1) In general. – Subject to paragraphs (2) and (3), the Secretary shall develop a mechanism, consistent with subchapter II of chapter 5 of title 5, United States Code, for an owner notified under subsection (b)(3) or for an owner that self-designates under subsection (b)(4) to request that the Secretary review

(A) the designation of a system or asset as covered critical infrastructure; or

(B) the rejection of an owner's self-designation of a system or asset as covered critical infrastructure or .

(2) Appeal to federal court. – A civil action seeking judicial review of a final agency action taken under the mechanism developed under paragraph (1) shall be filed in the United States District Court for the District of Columbia.

(3) Compliance. – The owner of a system or asset designated as covered critical infrastructure shall comply with this subtitle relating to covered critical infrastructure until such time as the system or asset is no longer designated as covered critical infrastructure, based on—

(A) an appeal under paragraph (1);

(B) a determination of the Secretary unrelated to an appeal; or

(C) a final judgment entered in a civil action seeking judicial review brought in accordance with paragraph (2).

Sec. 3. Advisory Standards, Guidelines and Widely Accepted Industry Practices

(a) The Director of the National Institute of Standards and Technology, in consultation with owners and operators of critical infrastructure and the National Cybersecurity Advisory Council, and in coordination with the Secretary, the Intelligence Community, the Department of Defense, the Department of Commerce, sector-specific agencies and other Federal agencies with responsibilities for regulating critical infrastructure companies, shall continue to participate in the development of information security standards, guidelines and widely accepted industry practices issued by private sector organizations, recognized international and domestic standards setting organizations, and Federal agencies.

(b) The advisory standards, guidelines, and widely accepted industry practices considered pursuant to subsection (a) should, as appropriate -

(1) address cybersecurity in a comprehensive, risk-based manner;

(2) address dynamic threat assessment and risk management practices;

(3) be suitable, as appropriate, for implementation by small business concerns;

(4) include consideration of the cost of implementing such widely accepted industry practices or of implementing recommended changes to standards and guidelines;

(5) as necessary and appropriate, be sector specific; and

(6) provide sufficient flexibility to permit a range of security solutions.

Sec. 4. Sector-by Sector Risk-Based Cybersecurity Performance Requirements

(a) The Secretary, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Committee, the National Cybersecurity Advisory Council, and appropriate information and analysis organizations, and in coordination with the National Institute of Standards and Technology, the Director of the National Security Agency, sector-specific agencies and other Federal agencies with responsibilities for regulating covered critical infrastructure, shall identify or develop, on a sector-by-sector basis, risk-based cybersecurity performance requirements that—

(1) Require owners of covered critical infrastructure to remediate or mitigate identified cyber risks and any associated consequences identified under section 1(a) or otherwise;

(2) ensure that personnel performing cybersecurity functions for covered critical infrastructure possess appropriate qualifications, which may include education, professional certifications, training, and experience; and

(3) as appropriate, may reflect the advisory standards, guidelines, and widely accepted industry practices considered in section 3.

(b) Where there are existing regulations that apply to a designated system or asset that address some or all of the risks identified under section 1, the Secretary shall only identify or develop risk-based cybersecurity performance requirements if the existing regulations do not require an appropriate level of security.

(c) In developing the risk-based cybersecurity performance standards, the Secretary shall identify existing widely accepted industry practices, standards, and guidelines, and shall to the extent practicable adopt or incorporate such best practices, standards, and guidelines, consistent with other provisions of this section.

(d) 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 an existing regulatory agency has sufficient specific requirements and enforcement mechanisms in place to effectively mitigate the risks identified under Section (1). The Secretary may reexamine any exemptions as appropriate.

(e) The Secretary, in developing the risk-based cybersecurity performance requirements shall take into consideration available resources, and anticipated consequences.

(f) Content of Risk Based Performance Requirements—

(1) Purpose – To promote and protect private sector innovation in design and development of technology for the global market for commercial information technology products, including hardware and software and related products and services.
(2) Limitation – The performance requirements developed under this section shall not permit any Federal employee or agency to:
(A) Regulate commercial information technology products, including hardware and software and related services, including installation services, maintenance

services, repair services, training services, and any other services provided in support of the product;
(B) Require commercial information technology products, including hardware and software and related services, for use or non-use in covered critical infrastructure; or
(C) Regulate the design, development, manufacturing or attributes of commercial information technology products, including hardware and software and related services, for use or non-use in covered critical infrastructure.

Sec. 5. Security of Covered Critical Infrastructure

(a) In general.—Not later than one year after the date of enactment of this subtitle, the Secretary, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Committee, and the National Cybersecurity Advisory Council, and in coordination with sector-specific agencies and other Federal agencies with responsibilities for regulating covered critical infrastructure, shall issue interim final rules to enhance the security of covered critical infrastructure against cyber risks

(b) Responsibilities.—The rules issued under this subsection shall establish procedures under which—

(1) owners of covered critical infrastructure—

(A) are regularly informed of cyber risk assessments, identified cybersecurity threats, and the risk-based security performance requirements appropriate to their sector established under section 4;

(B) select and implement the cybersecurity measures they determine to be best suited to satisfy the risk-based cybersecurity performance requirements established under section 4;

(C) develop or update continuity of operations and response plans including plans for a national cyber emergency declared under section 9; and

(D) shall report, consistent with the protections in section 7, significant cyber incidents affecting covered critical infrastructure.

(2) the Secretary—

(A) in consultation with the Federal agency with responsibilities for regulating covered critical infrastructure is notified of the security measure or measures selected by the owner of covered critical infrastructure pursuant to subparagraph (b)(1)(B);

(B) identifies, with owners and operators of covered critical infrastructure, cyber risks that are not capable of effective remediation or mitigation using available standards, widely accepted industry practices or other available security measures;

(C) provides owners of covered critical infrastructure the opportunity to develop practices or security measures to remediate or mitigate the cyber risks identified in section 1 without the prior approval of the Secretary and without affecting the

compliance of the covered critical infrastructure with the requirements under this section; and

(D) in accordance with applicable law relating to the protection of trade secrets, permits owners and operators of covered critical infrastructure to report to the Secretary the development of effective practices or security measures to remediate or mitigate the cyber risks identified under section 1.

(E) shall develop, in conjunction with the Secretary of Defense and the Director of National Intelligence and in coordination with the owners and operators of covered critical infrastructure, a procedure for ensuring that owners and operators of covered critical infrastructure are, to the maximum extent practicable and consistent with the protection of sources and methods, informed of relevant real-time threat information.

(c) Enforcement.—

(1) Requirements.—The rules issued under this subsection shall establish procedures that –

(A) require each owner of covered critical infrastructure –

(i) to certify annually in writing to the Secretary and the head of the Federal agency with responsibilities for regulating the covered critical infrastructure whether the owner has developed and effectively implemented security measures sufficient to satisfy the risk-based security performance requirements established under subsection 4; or

(ii) to submit annually a third-party assessment pursuant to subsection d;

(B) provide for civil penalties for any person who violates this section or section 9 and who fails to remediate such violation in an appropriate timeframe; and

(C) do not confer upon any person, except the Federal agency with responsibilities for regulating the covered critical infrastructure and the Secretary, a right of action against an owner or operator of covered critical infrastructure to enforce any provision of this section or section 9.

(2) Proposed security measures.—The owners of covered critical infrastructure may select any security measure or measures that satisfy the risk-based security performance requirements established under section 4.

(3) Recommended security measures.—Upon request from an owner or operator of covered critical infrastructure, the Secretary may recommend a specific security measure that the Secretary believes will satisfy the risk-based security performance requirements established under section 4.

(4) Security and performance-based exemptions.–

(A) The Secretary shall develop a process for an owner of covered critical infrastructure to demonstrate that a covered system or asset is sufficiently secured against the risks identified in Section 1, or that compliance with risk based performance requirements developed under section 4 would not substantially improve the security of the system or asset.

(B) Upon a finding by the Secretary that a covered system or asset is sufficiently secured against the risks identified in Section 1, or that compliance with risk based performance requirements developed under section 4 would not substantially improve the security of the system or asset, the owner shall not be required to select or implement cybersecurity measures or submit an annual certification or third party assessment as required under this Act.

(C) The Secretary shall require the owner of an exempted system or asset to demonstrate that it is sufficiently secured against the risks identified in Section 1, or that compliance with risk based performance requirements developed under section 4 would not substantially improve the security of the system or asset every three years, or if the Secretary has reason to believe that a system or asset no longer qualifies for such a finding.

(5) Enforcement Actions.—An action to enforce any regulation promulgated pursuant to this section or section 9 shall be initiated by –

(A) the Federal agency with responsibilities for regulating the covered critical infrastructure, in consultation with the Secretary; or

(B) the Secretary, when –

(i) the covered critical infrastructure is not subject to regulation by another Federal agency;

(ii) the head of the Federal agency with responsibilities for regulating the covered critical infrastructure requests the Secretary take such action; or

(iii) the Federal agency with responsibilities for regulating the covered critical infrastructure fails to initiate such action after a request by the Secretary.

(d) Assessments.—

(1) Third Party Assessments.—The rules issued under this subsection shall establish procedures for third party private entities to conduct assessments that utilize reliable, repeatable, performance-based evaluations and metrics to—

(A) assess the private sector companies' implementation of their selected security measures;

(B) assess the effectiveness of the security measure or measures implemented by the covered critical infrastructure in satisfying the risk-based security performance requirements established under section 4;

(C) require that third party assessors—

(i) be certified by the Secretary, in consultation with the head of any Federal agency with responsibilities for regulating covered critical infrastructure, after completing a proficiency program established by the Secretary in consultation with owners and operators of critical infrastructure and the National Cybersecurity Advisory Council, the Critical Infrastructure Partnership and Advisory Committee and in coordination with the Director of the National

Institute of Standards and Technology and relevant federal agencies;

(ii) undergo regular retraining and certification;

(iii) provide their findings with the owners and operators of covered critical infrastructure before submission to the government; and

(iv) submit their independent assessments to the owner of the covered critical infrastructure, the Secretary and to the federal agency with responsibilities for regulating the covered critical infrastructure.

(2) Other Assessments.—The rules issued under this subsection shall establish procedures under which the Secretary—

(A) may perform cybersecurity assessments of selected covered critical infrastructure, in consultation with relevant agencies, based on –

(i) the specific cyber risks affecting or potentially affecting the information infrastructure of the specific system or asset constituting covered critical infrastructure;

(ii) any reliable intelligence or other information indicating a cyber risk or credible national cyber emergency to the information infrastructure of the specific system or asset constituting covered critical infrastructure;

(iii) actual knowledge or reasonable suspicion that the owner of covered critical infrastructure is not in compliance with risk-based security performance requirements established under section 4; or

(iv) such other risk-based factors as identified by the Secretary.

(B) uses the resources of any relevant Federal agency with the concurrence of the head of such agency;

(C) uses existing government and private sector information security assessment programs to conduct assessments; and

(D) provides copies of any government assessments to the owner of the covered system or asset.

(3) Access to information.—

(A) For the purposes of an assessment under paragraphs (1) or (2) of subsection (b), an owner or operator of covered critical infrastructure shall provide an assessor any reasonable access necessary to complete an assessment under this section.

(B) Information provided to the Secretary, the Secretary's designee, or any assessor during the course of an assessment under this subsection shall be protected from disclosure in accordance with section 7.

(e) Limitations on civil liability.—

(1) In General.—In any civil action for damages directly caused by an incident related to a cyber risk identified under section 1(b), an owner or operator of covered critical infrastructure shall not be liable for any punitive damages intended to punish or deter

provided the owner or operator –

(i) has implemented security measures, or a combination thereof, that satisfy the security performance requirements established under section 4;

(ii) has undergone successful assessments, submitted an annual certification required by section 5, or been granted an exemption pursuant to section 5(c)(4); and

(iii) is in substantial compliance with the appropriate risk based cybersecurity performance requirements at the time of the incident related to that cyber risk.

(2) Limitation.—This subsection shall only apply to harm directly caused by the incident related to the cyber risk and shall not apply to damages caused by any additional or intervening acts or omissions by the covered entity.

Sec. 6. Sector Specific Agencies

(a) In General.—The head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure shall coordinate with the Secretary on any activities of the sector-specific agency or Federal agency that relate to the efforts of the agency regarding security or resiliency of critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

(b) Duplicative Reporting Requirements.—

(1) The Secretary shall coordinate with the head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure to determine whether existing reporting requirements substantially fulfill any reporting requirements called for under this title. Where such a report exists, the Secretary shall if at all practicable use that report to satisfy the reporting requirement under this title and shall require no further report.

(2) The Secretary shall coordinate with the head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure to eliminate any duplicate reporting or compliance requirements relating to the security or resiliency of critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

(c) Requirements.—

(1) In general.—To the extent that the head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure has the authority to establish regulations, rules, or requirements or other required actions that are applicable to the security of critical infrastructure and covered critical infrastructure, the head of that agency shall—

(A) notify the Secretary in a timely fashion of the intent to establish the regulations, rules, requirements, or other required actions;

(B) coordinate with the Secretary to ensure that the regulations, rules, requirements, or

other required actions are consistent with, and do not conflict or impede, the activities of the Secretary under this title; and

(C) in coordination with the Secretary, ensure that the regulations, rules, requirements, or other required actions are implemented, as they relate to covered critical infrastructure, in accordance with subsection (a).

(2) Rule of construction.—Nothing in this section shall be construed to provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating critical infrastructure or covered critical infrastructure, to establish standards or other measures that are applicable to the security of critical infrastructure not otherwise authorized by law.

Sec. 7. Protection of Information

(a) Definition.—In this section, the term 'covered information'—

(1) means—

(A) any information that constitutes a privileged or confidential trade secret or commercial or financial information that is appropriately marked at the time it is provided by owners and operators of critical infrastructure in sector-by-sector risk assessments conducted under section 1;

(B) any information required to be submitted under section 5 by the owners and operators of covered critical infrastructure; and

(C) any information submitted by State and local governments, private entities, and international partners of the United States regarding threats, vulnerabilities, and incidents affecting—

(i) the Federal information infrastructure;

(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

(iii) the critical infrastructure; and

(2) shall not include any information described under paragraph (1), if that information is submitted to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a person, organization, or agency; or

(C) interfere with competition in the private sector.

(b) Voluntarily Shared Critical Infrastructure Information.—Covered information submitted in accordance with this section shall be treated as voluntarily shared critical infrastructure information under section 214 of the Homeland Security Act, except that the requirement of section 214 that the information be voluntarily submitted, including the requirement for an express statement, shall not be required for submissions of covered information.

(c) Guidelines.—

(1) In general.—Subject to paragraph (2), the Secretary shall develop and issue guidelines, in consultation with the Secretary, Attorney General, the Critical Infrastructure Partnership Advisory Council and the National Cybersecurity Advisory Council, as necessary to implement this section.

(2) Requirements.—The guidelines developed under this section shall—

(A) include provisions for the sharing of information among governmental and nongovernmental officials and entities in furtherance of carrying out the authorities and responsibilities of the Secretary;

(B) be consistent, to the maximum extent possible, with policy guidance and implementation standards developed by the National Archives and Records Administration for controlled unclassified information, including with respect to marking, safeguarding, dissemination and dispute resolution; and

(C) describe, with as much detail as possible, the categories and type of information entities should voluntarily submit.

(d) Process for Reporting Security Threats, Vulnerabilities, and Incidents.—

(1) Establishment of process.—The Secretary shall establish through regulation, and provide information to the public regarding, a process by which any person may submit a report to the Secretary regarding cybersecurity threats, vulnerabilities, and incidents affecting—

(A) the Federal information infrastructure;

(B) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

(C) critical infrastructure.

(2) Acknowledgment of receipt.—If a report submitted under paragraph (1) identifies the person making the report, the Secretary shall respond promptly to such person and acknowledge receipt of the report.

(3) Steps to address problem.—Consistent with existing authority, the Secretary shall review and consider the information provided in any report submitted under paragraph (1) and, at the sole, unreviewable discretion of the Secretary, determine what, if any, steps are necessary or appropriate to address any threats, vulnerabilities, and incidents identified.

(4) Disclosure of identity.—

(A) In general.—Except as provided in subparagraph (B), or with the written consent of the person, the Secretary may not disclose the identity of a person who has provided information described in paragraph (1).

(B) Referral to the attorney general.—The Secretary shall disclose to the Attorney General the identity of a person described under subparagraph (A) if the matter is

referred to the Attorney General for enforcement. The Secretary shall provide reasonable advance notice to the affected person if disclosure of that person's identity is to occur, unless such notice would risk compromising a criminal or civil enforcement investigation or proceeding.

(e) Rules of Construction.—Nothing in this section shall be construed to—

(1) limit or otherwise affect the right, ability, duty, or obligation of any entity to use or disclose any information of that entity, including in the conduct of any judicial or other proceeding;

(2) prevent the classification of information submitted under this section if that information meets the standards for classification under Executive Order 12958 or any successor of that order or affect measures and controls relating to the protection of classified information as prescribed by Federal statute or under Executive Order 12958, or any successor of that order;

(3) limit the right of an individual to make any disclosure—

(A) protected or authorized under section 2302(b)(8) or 7211 of title 5, United States Code;

(B) to an appropriate official of information that the individual reasonably believes evidences a violation of any law, rule, or regulation, gross mismanagement, or substantial and specific danger to public health, safety, or security, and that is protected under any Federal or State law (other than those referenced in subparagraph (A)) that shields the disclosing individual against retaliation or discrimination for having made the disclosure if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

(C) to the Special Counsel, the inspector general of an agency, or any other employee designated by the head of an agency to receive similar disclosures;

(4) prevent the Secretary from using information required to be for enforcement of this subtitle, including enforcement proceedings subject to appropriate safeguards;

(5) authorize information to be withheld from Congress, the Comptroller General, or Inspector General of the Department;

(6) affect protections afforded to trade secrets under any other provision of law; or

(7) create a private right of action for enforcement of any provision of this section.

(f) Audit.—

(1) In general.—Not later than 1 year after the date of enactment of the, the Inspector General of the Department shall conduct an audit of the management of information submitted under subsection (b) and report the findings to appropriate committees of Congress.

(2) Contents.—The audit under paragraph (1) shall include assessments of—

(A) whether the information is adequately safeguarded against inappropriate

disclosure;

(B) the processes for marking and disseminating the information and resolving any disputes;

(C) how the information is used for the purposes of this section, and whether that use is effective;

(D) whether information sharing has been effective to fulfill the purposes of this section;

(E) whether the kinds of information submitted have been appropriate and useful, or overbroad or overnarrow;

(F) whether the information protections allow for adequate accountability and transparency of the regulatory, enforcement, and other aspects of implementing this subtitle; and

(G) any other factors at the discretion of the Inspector General.

Sec. 8. Voluntary Technical Assistance

Subject to the availability of resources, in accordance with applicable law relating to the protection of trade secrets, and at the discretion of the Secretary, the Secretary shall provide voluntary technical assistance—

(a) at the request of an owner or operator of covered critical infrastructure, to assist the owner or operator in meeting the requirements of sections 5 and 9, including implementing required security or emergency measures, restoring the critical infrastructure in the event of destruction or serious disruption, and developing response plans for national cyber emergencies declared under section 9; and

(b) at the request of the owner or operator of critical infrastructure that is not covered critical infrastructure, and based on risk, to assist the owner or operator in implementing widely accepted industry practices, and related standards and guidelines, recommended under section 3 and in response to other requests.

Sec. 9. Emergency Planning

Emergency planning. In partnership with owners and operators of covered critical infrastructure, the Secretary, in coordination with the heads of sector-specific agencies and the heads of other Federal agencies with responsibility for regulating covered critical infrastructure, shall exercise response and restoration plans, including plans required under section 5(b) to–

(a) assess performance and improve the capabilities and procedures of government and private sector entities to respond to a declaration under this section; and

(b) clarify specific roles, responsibilities, and authorities of government and private sector entities when responding to a declaration under this section.

Sec. 10. International Cooperation

(a) The Secretary, in coordination with the head of the sector-specific agencies and the head of any federal agency with responsibility for regulating covered critical infrastructure, shall—

(1) Consistent with the protection of intelligence sources and methods and other sensitive matters, inform the owner or operator of information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage within the United States and the government of the country in which the information infrastructure is located of any cyber risks to such information infrastructure or of the declaration of a national cyber emergency affecting such information infrastructure;

(2) Coordinate with the government of the country in which such information infrastructure is located and, as appropriate, the owner or operator of the information infrastructure regarding the implementation of security measures or other measures to the information infrastructure to mitigate or remediate cyber risks or to respond to the national cyber emergency.

(b) International Agreements.—The Secretary shall perform the functions prescribed by this section consistent with applicable international agreements.

Sec. 11. Effect On Other Laws.—

(a) Preemption of State Cybersecurity Laws.—This Act supersedes any statute, provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly requires comparable cybersecurity practices to protect a designated system or asset of covered critical infrastructure.

(b) Preservation of Other State Law.—Except as expressly provided in subsection (a) and Section 5(e), nothing in this Act shall be construed to preempt the applicability of any other state law or requirement.