TITLE XX: [PROTECTING CRITICAL INFRASTRUCTURE]

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

The Secretary of Homeland Security, in consultation with owners and operators of critical infrastructure 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 critical infrastructure companies shall –

(a) conduct, on an ongoing, sector-by-sector basis, cyber risk assessments of the national information infrastructure in a manner that –

(1) utilizes state-of-the art 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 a disruption of the reliable operation of critical infrastructure;

(C) the threat to or impact on national security caused by a disruption of the reliable operation of critical infrastructure;

(D) the extent to which the disruption of the reliable operation of critical infrastructure will disrupt the reliable operation of other critical infrastructure;

(E) the harm to the economy that would result from a disruption of the reliable

operation of critical infrastructure;

(F) the risk of national or regional catastrophic damage within the United States caused by the disruption of 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 subsection (b).

(c) The Secretary and the Director of the National Institute of Standards and Technology, in consultation with 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.

Sec. 2. Procedure for Designation of Covered Critical Infrastructure

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

(1) In General.--The Secretary 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) consult with owners and operators of critical infrastructure, 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; and

(C) periodically review and update designations under this section.

(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) only designate a system or asset as covered critical infrastructure if, through exploitation of a cyber vulnerability, the destruction or disruption of, 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; 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; or

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

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

(2) Limitation.—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.

(3) Identification of system or asset.—The Secretary shall promptly notify the owner or operator of any system or asset designated as covered critical infrastructure under the process established in this section.

(4) System or asset no longer covered critical infrastructure.—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 or operator of that system or asset of that determination.

(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 or operator notified under subsection (b)(3) to appeal the identification of a system or asset as covered critical infrastructure under this section.

(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 or operator of a system or asset identified as covered critical infrastructure shall comply with any requirement of this subtitle relating to covered critical infrastructure until such time as the system or asset is no longer identified 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 Best 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 review, assist in the development of, and recommend changes to information security standards, guidelines and best practices issued by private sector organizations, recognized international and domestic standards setting organizations, and Federal agencies.

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

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

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

(3) include consideration of the cost of implementing such best practices or of implementing recommended changes to standards and guidelines;

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

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

(c) The guidelines and best practices considered pursuant to subsection (a) should include those that address lifecycle management, product assurance, and supply chain risk management through the –

(1) assessment of risk from vendors;

(2) management of the quality and security of software, hardware, or systems, including components or subcomponents, throughout the lifecycle of the product or system;

(3) detection of the occurrence, reduction of the likelihood of the occurrence, and mitigation or remediation of risks associated with products containing counterfeit components or malicious functions; and

(4) enhancement of capabilities to test and evaluate software and hardware vulnerabilities.

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

The Secretary, in consultation with owners and operators of critical infrastructure and the National Cybersecurity Advisory Council, 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 the covered critical infrastructure, shall develop, on a sector-by-sector basis, risk-based cybersecurity performance requirements that—

(a) remediate or mitigate identified cyber risks and any associated consequences identified under section 1(b) or otherwise;

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

(c) require, the owner or operator of covered critical infrastructure to report, consistent with the protections in section 6, significant cyber incidents affecting covered critical infrastructure; and

(d) as appropriate, may reflect the advisory standards, guidelines, and best practices considered in section 3.

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 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 and operators of covered critical infrastructure—

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

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

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

(2) the Secretary—

(A) in consultation with the Federal agency with responsibilities for regulating covered critical infrastructure—

(i) is notified of the security measure or measures selected by the owner or operator of covered critical infrastructure pursuant to subparagraph (b)(1)(B); and

(ii) determines whether the proposed cybersecurity measure or measures satisfy the risk-based security performance requirements established pursuant to section 4;

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

(C) provides owners and operators of covered critical infrastructure the opportunity to develop best practices or security measures to remediate or mitigate the cyber risks identified in section (B) 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 best practices or security measures to remediate or mitigate the cyber risks identified under section 1.

(c) Assessments.—

(1) Third Party Assessments.—The rules issued under this subsection shall establish procedures for third party private entities to conduct periodic assessments, no less than annually, 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, and in coordination with the Director of the National Institute of Standards and Technology and relevant federal agencies;

(ii) do not provide remediation or consulting services to the owner or operator of the covered critical infrastructure;

(iii) undergo regular retraining and certification; and

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

[Inclusion of this subparagraph is subject to ongoing staff discussions.]

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

(A) performs 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 or operator 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; and

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

(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 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.

(d) Enforcement.—

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

(A) require each owner or operator of covered critical infrastructure 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 or operator has developed and implemented security measures sufficient to satisfy the risk-based security performance requirements established under subsection 4;

(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 and operators 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.—The Secretary may recommend to an owner and operator of covered critical infrastructure a specific security measure that the Director believes will satisfy the risk-based security performance requirements established under section 4.

(4) Limitation.—The Secretary may not disapprove any proposed security measure or measures, based on the presence or absence of any particular security measure, including a security measure recommended under paragraph (3), if the security measure or measures proposed by the owner or operator of covered critical infrastructure otherwise satisfy the risk-based security performance requirements established under section 4.

(5) Determination.—A determination by the Secretary under subsection (b)(2) shall not

limit the obligation of an owner or operator of covered critical infrastructure to take all reasonable methods to secure the covered critical infrastructure.

(6) 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.

(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 –

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

(B) has undergone successful assessments required by section 5(b)(6); and

(C) is in actual compliance with the approved security measures 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.

[Inclusion of this subparagraph is subject to ongoing staff discussions.]

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 the national information infrastructure, including critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

(b) Duplicative Reporting Requirements.—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 and avoid the creation of duplicate reporting or compliance requirements relating to the security or resiliency

of the national information infrastructure, including 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 national information infrastructure, including 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 national information infrastructure, including critical infrastructure or covered critical infrastructure, to establish standards or other measures that are applicable to the security of national information 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 required to be submitted under section 5 by the owners and operators of covered critical infrastructure; and

(B) 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 national information 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, 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 Problems.—

(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) national information 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 problems or deficiencies 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 national information infrastructure that is not covered critical infrastructure, and based on risk, to assist the owner or operator in implementing best practices, and related standards and guidelines, recommended under section 3 and in response to other requests.

Sec. 9. Emergency Planning and Response

(a) 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–

(1) assess performance and improve the capabilities and procedures of government and

private sector entities to respond to a declaration under this section; and

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

(b) Declaration. The President may issue a declaration of cyber emergency if there is an actual or imminent action by an individual or entity with the capability and intent to exploit a cyber risk that could disrupt the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure. Any declaration under this section shall specify the covered critical infrastructure subject to the national cyber emergency.

(c) Notification to owners. Upon issuing a declaration, the President, through the Secretary and consistent with the protection of intelligence sources and methods, shall notify affected owners and operators of covered critical infrastructure and the relevant federal agencies and departments of the nature of the cyber emergency.

(d) Emergency measures.

(1) Responding to a cyber emergency. – Consistent with a declaration issued under subsection (b), the President, through the Secretary, shall –

(A) direct actions by other federal agencies to respond to the national cyber emergency;

(B) direct owners and operators to implement continuity of operations and response plans developed pursuant section 5(b);

(C) direct covered critical infrastructure to take such other emergency measures necessary to preserve the reliable operation, and mitigate the consequences of the potential disruption of the covered critical infrastructure that is the subject to the declaration. The emergency measures must be the least disruptive means feasible that ensure the reliable operation of the covered critical infrastructure and the national information infrastructure.

(D) Upon request of the owner or operator of covered critical infrastructure that is subject to the declaration and resources permitting, provide voluntary technical assistance to covered critical infrastructure to aid in the response to the national cyber emergency;

(E) coordinate with State and local governments, international partners, and other relevant private sector entities to respond to the national cyber emergency; and

(F) initiate a process under sections 4 and 5 to address the cyber risk that is the subject of the national cyber emergency.

(2) Recovering from a cyber emergency. -- The President may, consistent with applicable law, subsection (j), and depending on the type, duration, and consequences related to a cyber emergency, designate the head of a federal agency or department to lead the federal effort to recover from any such damages.

(e) Alternative measures.

(1) The President, acting through the Secretary, may approve alternative emergency measures proposed by owners and operators of covered critical infrastructure, provided that

they are at least as effective as those ordered.

(2) During a national cyber emergency, covered critical infrastructure required to implement an emergency measure under subsection (d) shall not be precluded from implementing additional security measures designed to remediate or mitigate the cyber risk or associated consequences to the extent such actions are not inconsistent with the emergency measure required to be implemented.

(f) Notification to Congress. Concurrent with the declaration of a national cyber emergency, the President shall submit to Congress:

(1) The circumstances necessitating the emergency declaration and emergency measures;

(2) The estimated scope and duration of the emergency; and

(3) A description of any ordered emergency measures.

(g) Discontinuance of emergency measures. Any emergency measure ordered under this section shall cease to have effect not later than 30 days after the date on which the President issued the declaration, unless the President issues a written order or directive reaffirming the emergency, the continuing nature of the emergency, or the need to continue the adoption of the emergency measure. The emergency measure may not be extended for more than 90 days without a joint resolution of Congress, provided that such resolution shall be considered in both the House and the Senate under rules that require a timely vote on acceptance or rejection of the resolution.

(h) Prohibited actions.—The authority to direct compliance with an emergency measure or action under this section shall not authorize the President, the Secretary, the Department, or any other Federal entity to—

(1) shut down the Internet;

(2) restrict or prohibit communications carried by, or over, covered critical infrastructure and not specifically directed to or from the covered critical infrastructure unless the Secretary determines that no other emergency measure or action will preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of the covered critical infrastructure or the national information infrastructure;

(3) control covered critical infrastructure;

(4) compel the disclosure of information unless specifically authorized by law;

(5) direct any entity to take any action or measure based solely on activities protected by the first amendment to the United States Constitution; or

(6) intercept a wire, oral, or electronic communication (as those terms are defined in section 2510 of title 18, United States Code), access a stored electronic or wire communication, install or use a pen register or trap and trace device, or conduct electronic surveillance (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.1801)) relating to an incident unless otherwise authorized under chapter 119, chapter 121, or chapter 206 of title 18, United States Code, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(i) Rule of Construction.—Nothing in this section shall be construed to—

(1) alter or supersede the authority of the Secretary of Defense, the Attorney General, or the

Director of National Intelligence in responding to a national cyber emergency;

(2) limit the authority of the Secretary of Homeland Security or the Administrator of the Federal Emergency Management Agency under the Homeland Security Act or the Robert T. Stafford Act in responding to or recovering from natural disasters, acts of terrorism, or other man-made disasters; or

(3) limit the authority of the Secretary under section 5 after a declaration under this section expires.

(j) Statutory Defenses and Civil Liability Limitations for Compliance With Emergency Measures.—A civil action may not be maintained against an owner or operator of covered critical infrastructure for harm that is the direct consequence of actions taken in good faith for the purpose of implementing specific emergency measures or actions directed pursuant to subsection (d)(1)(C), if the owner or operator is in compliance with the emergency measures required under the subsection and the harm was not caused by an intervening act or omission by the owner or operator.

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.