SEC. 101. DEFINITIONS.—In this Act:

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

(2) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given the term in section 2209 of the Homeland Security Act of 2002.

(3) DEPARTMENT.—The term "Department" means the Department of Homeland Security.

(4) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(5) DIRECTOR.—The term "Director" means the National Cyber Director.

(6) SECTOR RISK MANAGEMENT AGENCY.—The term "Sector Risk Management Agency" has the meaning given that term is section 2201 of the Homeland Security Act of 2002.

(7) SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—The term "systemically important critical infrastructure" means a facility, system, or asset, either alone or in combination, that has been designated as systemically important critical infrastructure pursuant to the requirements of this Act.

(8) CLOUD SERVICE PROVIDER.—The term "cloud service provider" means any nongovernmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit, that provides on-demand availability of computer system resources, such as computing power or data storage.

(9) SERVICE PROVIDER.— The term "service provider" means:

(A) a nongovernmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit, that provides digital data transmission, routing, storage, or connections to its system or network, where the entity providing such services does not select or modify the content of the digital data and is not the sender or the intended recipient of the data; or

(B) a cloud service provider.

(10) National Critical Functions.—The term "national critical functions" means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

(11) Covered Entities.—The term "covered entities" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit, that owns or operates a facility, system, or asset, either alone or in combination, that is designated as systemically important critical infrastructure pursuant to requirements of this Act.

(12) Federal agency with responsibilities for regulating the security of critical infrastructure.—The term "Federal agency with responsibilities for regulating the security of critical infrastructure" means

SEC. 102. PROCEDURE FOR DESIGNATION OF COVERED SYSTEMICALLY IMPORTANT SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.

(a) Responsibility For Designation Of Covered Systemically Important Critical Infrastructure.—

(1) Procedures.—No later than 12 months after the date of enactment of this Act, and no less often than every four years thereafter, the Secretary, in consultation with Sector Risk Management Agencies, the Director, and the Critical Infrastructure Partnership Advisory Council, shall establish procedures for the designation of critical infrastructure as systemically important critical infrastructure for the purposes of this Act.

(2) Elements.—In establishing the procedure under paragraph (1), the Secretary shall develop a mechanism for owners or operators of critical infrastructure to submit information to assist the Secretary in making determinations under this section;

(b) Designation Of Systemically Important Critical Infrastructure.— The Secretary shall, on a rolling basis and using the procedures established pursuant to

paragraph (a)(1), designate entities as systemically important critical infrastructure based on the consequences an entity's impairment would have on one or more national critical functions.

(1) NOTIFICATION OF IDENTIFICATION OF SYSTEM OR ASSET.—Not later than 30 days after the Secretary designates a function, facility, system, or asset as systemically important critical infrastructure under this section, the Secretary shall notify each covered entity of the facility, system, or asset that was designated and the basis for the designation.

(2) NOTIFICATION OF DESIGNATION TO SERVICE PROVIDERS.—Not later than 30 days after the Secretary designates a facility, system, or asset as systemically important critical infrastructure under this section, the Secretary shall notify service providers of the names of covered entities that own or operate facilities, systems, or assets designated as systemically important critical infrastructure.

(3) FACILITY, SYSTEM, OR ASSET NO LONGER COVERED AS SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—The Secretary shall review the register established pursuant to subparagraph (4) not less frequently than every 12 months to and make a redetermination of each listed facility, system, or asset.

> (A) If the Secretary determines that any facility, system, or asset that was designated as systemically important critical infrastructure under this section no longer constitutes systemically important critical infrastructure, the Secretary shall promptly notify the relevant covered entity and service providers.

(4) SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE REGISTER.—The Secretary shall maintain and routinely update a list, or "register", of each facility, system, or asset designated as systemically important critical infrastructure, each covered entity responsible for ownership or operation, means to contact each entity, and, where applicable, each individual serving as a point of contact for such an entity.

(5) REGISTER CLASSIFICATION.—With the exception of the names of covered entities which shall not be classified**,** the Secretary may classify any part of the register established pursuant to (b)(6) of this section in the interest of national security or

any item related to systemically important critical infrastructure designated for reasons listed under (b)(1)(C)(iii) of this section.

(c) LIMITATIONS.—

(1) IN GENERAL.—The number of designated covered entities who own or operate facilities, systems, or assets designated as systemically important critical infrastructure pursuant to this Act shall not exceed 120 in total.

(2) SUNSET.—Beginning on the date that is four years after the date of enactment of this Act, the Secretary, after consultation with the Director, may increase the number of covered entities provided:

(A) The number of covered entities does not exceed 150 percent of the prior maximum.
(B) The Secretary publishes the new maximum number in the Federal Register.
(C) The new maximum number has not been changed in the past four years.

(d) 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 a covered entity notified under subsection (b)(3) or (4) to present evidence that the Secretary should reverse—

(A) the designation of a facility, system, or asset as covered systemically important critical infrastructure; or

(B) the determination that a facility, system, or asset no longer constitutes systemically important 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.—A covered entity shall comply with the requirements of this Act relating to systemically important critical infrastructure until such time as the

facility, system, or asset is no longer designated as systemically important 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. 103. PERFORMANCE STANDARDS

(a) SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE OVERSIGHT COUNCIL--There is established a Systemically Important Critical Infrastructure Oversight Council

(b) STRUCTURE OF THE COUNCIL-

(1) CHAIR--THE Secretary of Homeland Security shall serve as the chairperson of the Council.

(2) ADDITIONAL MEMBERSHIP--Each of the sixteen sectors of critical infrastructure shall be represented on the Systemically Important Critical Infrastructure Oversight Council with one vote. That vote shall be cast-

(A) By the head of the Federal agency with responsibility for regulating the security of a given sector of critical infrastructure, if only one such agency exists for that sector; or

(B) By one of the heads of the Federal agencies with responsibility for regulating the security of a given sector of critical infrastructure, in coordination with the heads of the other such agencies with responsibility for the security of the same sector.

(3) ACTING OFFICIALS--In the event of a vacancy in the office of the head of a member agency, and pending the appointment of a successor, or during the absence or disability of the head of a member agency or department, the acting head of the member agency shall vote on the Council in the place of that agency or department head.

(c) Timing.—The Council shall meet at the call of the Chairperson or a majority of the members then serving, but not less frequently than quarterly.

(d) Voting--Unless otherwise specified, the Council shall make all decisions that it is authorized or required to make by a majority vote of the voting members then serving.

(e) Assistance from Federal Agencies--Any department or agency of the United States may provide to the Council and any special advisory, technical, or professional committee appointed by the Council, such services, funds, facilities, staff, and other support services as the Council may determine advisable.

(f) Compensation of Members--

(1) Federal Employee Members -- All members of the Council who are officers or employees of the United States shall serve without compensation in addition to that received for their services as officers or employees of the United States.

(g) Purposes and Duties of the Council--

(1) Purposes-- In order to prevent the severe consequences to one or more national critical functions that could arise from the compromise of systemically important critical infrastructure, the Council shall--

(A) Identify cybersecurity risks to systemically important critical infrastructure

(B) Develop, based on those cybersecurity risks, cybersecurity performance standards for owners and operators of systemically important critical infrastructure that--

(i) Are applicable to all entities who own or operate systemically important critical infrastructure, regardless of the critical infrastructure sector to which such entities belong or the specific technologies used by such entities

(ii) Are more stringent than those applicable to entities who do not own or operate systemically important critical infrastructure

(iii) Incorporate existing industry best practices, standards, and guidelines to the greatest extent possible

(C) On a non-delegable basis and by a majority vote, including an affirmative vote by the Chairperson, promulgate the cybersecurity performance standards specified by subparagraph (B)

(2) OTHER DUTIES-- The Council shall, in accordance with this paragraph--

(A) Collect information from member agencies, appropriate Information Sharing and Analysis Organizations, Sector Risk Management Agencies, the Critical Infrastructure Partnership Advisory Council, the Director of the National Security Agency, appropriate representatives from State and local governments, the National Institute of Standards and Technology, and owners and operators of systemically important critical infrastructure, and if necessary, direct the Cybersecurity and Infrastructure Security Agency to collect such information.

(B) Provide direction to, and request data and analysis from, the Cybersecurity and Infrastructure Security Agency to support the work of the Council;

(C) Monitor for and identify potential cybersecurity threats to the systemically important critical infrastructure of the United States;

(D) Facilitate information sharing and, where applicable, coordination among the member agencies regarding cybersecurity policy development, rulemaking, examinations, reporting requirements, and enforcement actions

(E) Recommend to the member agencies general supervisory priorities and principles reflecting the outcome of discussions among the member agencies;

(F) Identify gaps in regulation that could invite cybersecurity risks to the systemically important critical infrastructure of the United States.

(G) Make non-binding recommendations to member agencies to apply new or heightened technical measures to mitigate security risks to systemically important critical infrastructure.

(H) Provide a forum for discussion and analysis of emerging cybersecurity developments and regulatory issues; and

(I) Annually report to and testify before Congress on--

(i) the activities of the Council;

(ii) Significant cybersecurity developments, including potential emerging cybersecurity threats or vulnerabilities, that pose risk to United States systemically important critical infrastructure

(iii) Recommendations to enhance the cybersecurity and resilience of the systemically important critical infrastructure of the United States.

(h) TESTIMONY BY THE CHAIRPERSON-- The Chairperson shall appear before the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate at an annual hearing, after the report is submitted under paragraph (2)--

(1) to discuss the efforts, activities, objectives, and plans of the Council; and

(2) to discuss and answer questions concerning such report.

(i) AUTHORITY TO OBTAIN INFORMATION–

(1) IN GENERAL-- The Council may receive, and may request the submission of, any data or information from the Cybersecurity and Information Security Agency, or other sources named in subparagraph (2)(A) as necessary to carry out the purposes and duties described in this subsection.

(2) REPORTS--

(A) IN GENERAL--Subject to subparagraph (2)(B) of this subsection, the Council, acting through the Cybersecurity and Infrastructure Security Agency, may require an entity who owns or operates systemically important critical infrastructure to submit reports to keep the Council informed as to--

(i) The cybersecurity policies and controls put in place to mitigate risks, including cybersecurity risks, to the systemically important critical infrastructure under their control.

(ii) Critical technologies or dependencies within such entity's supply chain that support the continued operation of the systemically important critical infrastructure under the entity's control, including, where possible, a Software Bill of Materials.

(iii) Policies and controls put in place to mitigate risk to the systemically important critical infrastructure under the entity's control emanating from the entity's supply chain

(iv) The extent to which the systemically important critical infrastructure under the entity's control supports one or more national critical functions

(B) USE OF EXISTING REPORTS-

(i) IN GENERAL-- For purposes of compliance with subparagraph (A), the Council, acting through the Cybersecurity and Infrastructure Security Agency, shall, to the fullest extent possible, use either publicly available reports or reports that an entity who owns or operates systemically important critical infrastructure has been required to provide to a Council member agency or to a relevant foreign supervisory authority

(ii) AVAILABILITY-- Each entity who owns or operates systemically important critical infrastructure shall provide to the Council, at the request of the Council, copies of all reports referred to in clause (i) of this subparagraph.

(j) Cybersecurity and Infrastructure Security Agency Support to the Council--

(1) In General-- The Cybersecurity and Infrastructure Security Agency shall support the Council in fulfilling the purposes and duties of the Council, as set forth in this section, and to support member agencies, by--

(A) Collecting data on behalf of the Council, and providing such data to the Council;

(B) Standardizing the types and formats of data reported and collected;

(C) Performing applied research and essential long-term research;

(D) Developing tools for risk measurement and monitoring;

(E) Performing other related services;

(F) Making the results of its activities available to member agencies; and

(G) Assisting such member agencies in determining the types and formats of data authorized by this Act to be collected by the Council

(2) Technical and Professional Advisory Committees--The Cybersecurity and Infrastructure Security Agency, in consultation with the Chairperson of the Council, may appoint such special advisory, technical, or professional committees as may be useful in carrying out the duties listed in paragraph (1), and the member of such committees may be staff of the Agency, or other persons, or both.

(3) Fellowship Program--The Cybersecurity and Infrastructure Agency, in consultation with the Chairperson, may establish and maintain an academic and professional fellowship program, under which qualified academic and professionals shall be invited to spend not longer than 2 years at the Agency, to perform research and to provide advanced training to Agency personnel.

(4) Testimony-- The Director of the Cybersecurity and Infrastructure Security Agency shall report to and testify before the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate on the activities of the Agency in support of the Council, as well as potential emerging threats to the systemically important critical infrastructure of the United States.

(k) Sector-specific Performance Standards.—The Secretary, with the concurrence of the relevant Sector Risk Management Agency and Federal agency with responsibility for regulating the security of that sector of critical infrastructure, may supplement the

performance standards identified or established pursuant to subsection (a) on a sector-by-sector basis to take into account sector-specific risks, challenges, or security concerns.

SEC. 104. SECURITY OF SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.

(a) IN GENERAL.—Not later than 12 months after the promulgation of new performance standards for systemically important critical infrastructure as described in Section 103 of this Act, the Secretary, in consultation with owners and operators, and the Critical Infrastructure Partnership Advisory Council, and in coordination with the Director, Sector Risk Management Agencies, and other Federal agencies with responsibilities for regulating the security of critical infrastructure, shall promulgate regulations to enhance the security of systemically important critical infrastructure against cyber risks.

(b) RESPONSIBILITIES.—The regulations promulgated under this section shall establish procedures under which each covered entity is required—

(1) to implement cybersecurity measures sufficient to satisfy the risk-based cybersecurity performance requirements developed pursuant to section 103 of this Act;

(2) to notify the Secretary and each Federal agency with responsibilities for regulating the security of critical infrastructure of the security measure or measures required under paragraph (1);

(3) to develop and update continuity of operations and cyber incident response plans;

(4) to certify, on an annual basis, in writing to the Secretary and the head of any Federal agency with responsibilities for regulating the security of critical infrastructure that the owner has developed and effectively implemented security measures sufficient to satisfy the risk-based security performance requirements established under section 103 of this Act.

(c) ENFORCEMENT.—

(1) IN GENERAL.—The regulations promulgated under this section—

(A) shall impose civil penalties for any person who violates this section; and

(B) shall not confer upon any person, except the Federal agency with responsibilities for regulating the security of covered entities and the Secretary, a right of action against an owner or operator to enforce any provision of this section.

(2) ENFORCEMENT ACTIONS.—An action to enforce any regulation promulgated pursuant to this section shall be initiated by—

(A) the Federal agency with responsibility for regulating the security of critical infrastructure, in consultation with the Secretary; or

(B) the Secretary, if —

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

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

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

(d) SECURITY AND PERFORMANCE-BASED EXEMPTIONS.—

(1) IN GENERAL.—The regulations promulgated under this section shall include a process for covered entities to demonstrate that compliance with risk-based performance requirements developed under section 103 of this Act would not substantially improve the security of the facility, system, or asset designated as systemically important critical infrastructure under this Act.

(2) EXEMPTION AUTHORITY.—Upon a determination by the Secretary that compliance with risk based performance standards developed under section 103 of this Act would not substantially improve the security of the facility, system or asset, the Secretary shall exempt the covered entity from the requirements to select or

implement cybersecurity measures or submit an annual certification required by this Act.

(3) RECURRENT DETERMINATION.—The Secretary shall require a covered entity that was exempted under paragraph (2) to demonstrate that compliance with risk-based performance standards developed under section 103 would not substantially improve the security of the facility, system, or asset—

(A) not less than once every 3 years; or

(B) at any time, if the Secretary has reason to believe that the relevant facility, system, or asset no longer meets the exemption qualifications under paragraph (2).

(e) OTHER ASSESSMENTS.—The regulations promulgated under this section shall establish procedures under which the Secretary—

(1) may perform cybersecurity assessments of selected covered entities, in consultation with relevant agencies, based on—

(A) the specific cyber risks affecting or potentially affecting the information infrastructure of the specific facility, system, or asset constituting systemically important critical infrastructure owned or operated by the covered entity;

(B) any reliable intelligence or other information indicating a cyber risk to the information infrastructure of the facility, system, or asset constituting systemically important critical infrastructure owned or operated by the covered entity;

(C) actual knowledge or reasonable suspicion that a covered entity is not in compliance with risk-based security performance requirements established under section 103 of this Act; or

(D) such other risk-based factors as identified by the Secretary; and

(2) may use the resources of any relevant Federal agency with the concurrence of the head of such agency;

(3) provides copies of any Federal Government assessments to the covered entity.

(f) ACCESS TO INFORMATION.—

(1) IN GENERAL.—For the purposes of an assessment conducted under subsection (e) paragraph (1) or (2), a covered entity shall provide an assessor any reasonable access necessary to complete the assessment.

(2) PROTECTION OF INFORMATION.—Information provided to the Secretary, the Secretary's designee, or any assessor during the course of an assessment under this section shall be protected from disclosure in accordance with section 106 of this Act.

SEC. 105. DUPLICATIVE REQUIREMENTS.

(a) IN GENERAL.—The head of each agency with responsibilities for regulating the security of critical infrastructure shall coordinate with the Secretary and the Director on any activities that relate to the efforts of the agency regarding the cybersecurity and resilience of covered entities, within or under the supervision of the agency.

(b) DUPLICATIVE REPORTING REQUIREMENTS.—

(1) IN GENERAL.—The Secretary shall coordinate with the head of any Federal agency with responsibilities for regulating the security of critical infrastructure to determine whether reporting requirements in effect on the date of enactment of this Act or subsequently enacted after such date substantially fulfill any reporting requirements required by this Act.

(2) PRIOR REQUIRED REPORTS.—If the Secretary determines that a report that was required under a regulatory regime in existence on the date of enactment of this Act substantially satisfies a reporting requirement under this title, the Secretary shall accept such report and may not require a covered entity to submit an alternate or modified report.

(3) COORDINATION.—The Secretary shall coordinate with the head of any Federal agency with responsibilities for regulating the security of critical infrastructure to eliminate any duplicate reporting or compliance requirements relating to the security or resiliency of covered entities.

(c) REQUIREMENTS.—

(1) IN GENERAL.—To the extent that the head of any Federal agency with responsibilities for regulating the security of critical infrastructure has the authority to establish regulations, rules, or requirements or other required actions that are applicable to the security of covered entities, the head of the agency shall—

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

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

(2) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authority for any Federal agency with responsibilities for regulating the security of critical infrastructure to establish standards or other measures that are applicable to the security of covered entities not otherwise authorized by law.

SEC. 106. 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 transaction that is appropriately marked at the time it is provided by covered entities;

(B) any information submitted by critical infrastructure owners and operators pursuant to section 102 of this Act;

(C) any information required to be submitted by owners and operators pursuant to section 104 of this Act;

(D) any information submitted by covered entities pursuant to section 111 of this Act;

(E) any information submitted by owners and operators pursuant to section 112 of this Act; and

(2) does 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 SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE INFORMATION.—Covered information submitted in accordance with this section shall be treated as voluntarily shared critical infrastructure information under section 2224 of the Homeland Security Act, except that the requirement of such section 2224 that the information be voluntarily submitted, including the requirement for an express statement, shall not be required for protection of information under this section.

(c) GUIDELINES.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall develop and issue guidelines, in consultation with the Director, Attorney General, the Critical Infrastructure Partnership Advisory Council, and appropriate Information Sharing and Analysis Organizations, 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 pursuant to this Act;

(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) 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 thereto, 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 thereto;

(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 or Federal agencies with the responsibility for regulation critical infrastructure from using information required to be submitted under this Act for enforcement of this title, including enforcement proceedings subject to appropriate safeguards;

(5) authorize information to be withheld from Congress, the Comptroller General, or the 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.

(e) AUDIT.—

(1) IN GENERAL.—Not later than 4 years after the date of enactment of this Act and every two years thereafter, the Inspector General of the Department shall conduct an audit of the management of information submitted under this section 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 overly narrow;

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

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

SEC. 107. VOLUNTARY TECHNICAL ASSISTANCE.

a121b

SEC. 108. EMERGENCY PLANNING.

(a) IN GENERAL.—In partnership with covered entities, the Secretary, in coordination with the Director, heads of Sector Risk Management Agencies, and the heads of other Federal agencies with responsibilities for regulating critical infrastructure, shall regularly exercise response, recovery, and restoration plans, including plans required under section 104(b) of this Act to—

(1) assess performance and improve the capabilities and procedures of government and private sector entities to respond to a major cyber incident; and

(2) clarify specific roles, responsibilities, and authorities of government and private sector entities when responding to a major cyber incident.

SEC. 109. LIMITATION OF LIABILITY.

(a) IN GENERAL.—Except as provided in subsection (b), no cause of action shall lie in any court against the covered entity for damages or harm directly or indirectly caused by a cyber incident, if the covered entity—

(1) has implemented security measures, or a combination thereof, that satisfy the security performance requirements established under section 103 of this Act;

(2) has submitted an annual certification as required by section 104(b), or been granted an exemption pursuant to section 104(d)(2);

(3) is in compliance with the appropriate risk-based cybersecurity performance requirements at the time of the incident related to that cyber risk;

(4) the relevant cyber incident was reported to the Director of the Cybersecurity and Infrastructure Security Agency.

(b) EXCEPTION.— The requirement under subsection (a)(4) shall not apply if the covered entity first discovered, or was otherwise first made aware of, the cyber incident through notification by a Federal department or agency.

(c) LIMITATION.—Paragraph (1) shall only apply to damages or harm directly or indirectly caused by the cyber incident and shall not apply to damages or harm caused by criminal or gross negligence.

SEC 110. DEPARTMENT OBLIGATIONS FOR INCIDENT RESPONSE

(a) IN GENERAL.—On discovering or receiving notice of a cyber incident affecting a covered entity, the Secretary shall—

(1) promptly establish contact with the affected covered entity to acknowledge receipt of notification, obtain additional information on the cyber incident, and ascertain need for incident response or technical assistance;

(2) maintain routine or continuous contact with the affected entity to monitor developments related to the incident; assist in incident response, mitigation, and recovery efforts; and ascertain evolving needs of the covered entity;

(3) prioritize voluntary incident response and technical assistance for the covered entity;

(4) promptly but no later than 14 days after discovering or receiving notice of a cyber incident affecting a covered entity, provide notice to other covered entities that are likely or are reasonably believed to be at-risk of being similarly compromised, targeted, or affected by a cyber incident; and

(5) preserve the anonymity and identity of the covered entity, consistent with section 106 of this Act and applicable laws and regulations.

(b) NATIONAL SECURITY AND LAW ENFORCEMENT EXEMPTION.—Notwithstanding subsection (a)(4), the Secretary may withhold notification to other covered entities—

(1) if the Secretary determines that withholding such information is in the national security interest of the United States; or

(2) at the request of the Director of National Intelligence, Attorney General, or head of a law enforcement agency and with the concurrence of the Secretary.

(c) Protection of Information.—Information disclosed to the Secretary or shared with covered entities pursuant to this section shall be considered "covered information" under section 106 of this Act.

(d) Notification to the Director.—In instances where the Secretary determines that a cyber incident affecting a covered entity is particularly severe or has, or is likely to, affect multiple covered entities, the Secretary shall promptly provide notice to the Director.

SEC. 111. INTELLIGENCE SUPPORT TO SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE

(a) In general.—Not later than 12 months after the date of enactment of this Act, the Director of National Intelligence, in coordination with the Secretary, Director, and appropriate Sector Risk Management Agencies shall establish a formal process to routinely provide intelligence support and indications and warning to covered entities.

(b) Interdependency and Risk Identification.—In developing and implementing the process under subsection (a), the Secretary shall incorporate methods and procedures—

(1) to identify the types of information needed to understand interdependence of systemically important critical infrastructure and areas where a nation-state adversary may target to cause widespread compromise or disruption, including—

(A) common technologies, including hardware, software, and services, used within covered entities;

(B) critical lines of businesses, services, processes, and functions on which multiple covered entities are dependent;

(C) specific technologies, components, materials, or resources on which multiple covered entities are dependent; and

(D) federal, state, local, tribal, or territorial government services, functions, and processes on which multiple covered entities are dependent; and

(2) to associate specific covered entities with the information identified under paragraph (1);

(c) INTELLIGENCE GAPS AND INDICATIONS AND WARNING.—In developing and implementing the process under subsection (a), the Director of National Intelligence shall incorporate methods and procedures—

(1) to provide indications and warning to covered entities regarding nation-state adversary cyber operations relevant to information identified under subsection (b)(1); and

(2) to identify intelligence gaps across covered entity cybersecurity efforts;

(d) RECURRENT INPUT.— Not later than 30 days following the establishment of the process required pursuant to subsection (a), and no less often than biennially thereafter, the Director of National Intelligence, in coordination with the Secretary, shall solicit information from covered entities utilizing the process established pursuant to subsection (a).

(e) INTELLIGENECE COLLECTION.—Utilizing the information received through the process established pursuant to subsection (a), as well as existing intelligence information and processes, the Director of National Intelligence, in coordination with the Secretary and in consultation with Sector Risk Management Agencies shall, to the greatest extent practicable, refocus information collection, analysis, and production activities as necessary to address identified gaps and mitigate threats to the cybersecurity of systemically important critical infrastructure of the United States.

(f) REQUIREMENT TO SHARE INTELLIGENCE INFORMATION WITH SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE.—

(1) IN GENERAL.— No later than 5 days after discovery of information that indicates a credible threat relevant to information identified in subsection (b)(1) or to an

identifiable covered entity, the Director of National Intelligence shall share the appropriate intelligence information with the relevant covered entity.

(2) EMERGENCY NOTIFICATION.—The Director of National Intelligence shall share any intelligence information related to a covered entity with such entity not later that 24 hours after the Director of National Intelligence determines that such information indicates an imminent threat—

(A) to a systemically important critical infrastructure facility, system, or asset the covered entity owns or operates;

(B) that is relevant to information identified in subsection (b)(1); or

(C) to national security, economic security, or public health and safety relevant to the covered entity.

(3) NATIONAL SECURITY EXEMPTIONS.—Notwithstanding paragraphs (1) or (2), the Director of National Intelligence may withhold intelligence information pertaining to a covered entity if the Director of National Intelligence, with the concurrence of the Secretary and the Director, determines that withholding such information is in the national security interest of the United States.

(4) PERIODIC REVIEW.—The Director of National Intelligence and the Secretary shall, in coordination with the Director, periodically, but no less often than every three months, conduct a review of information or intelligence withheld under paragraph (3) to—

(A) reevaluate the decision on withholding the information or intelligence in consideration of evolving threats, new circumstances, or newly-identified intelligence gaps;

(B) make a determination as to whether such information or intelligence shall continue to be withheld or shared with relevant covered entities pursuant to the process established in subsection (a); and

(C) document the determination, including the reasons for determinations made under subparagraph (B), for future periodic reviews.

(g) REPORT TO CONGRESS.—No later than 18 months after the date of enactment of this Act, and annually thereafter, the Director of National Intelligence, in coordination with the Secretary and in consultation with the Director, shall submit to the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Homeland Security of the House of Representatives a report that—

(1) assesses how the information obtained from covered entities is shaping intelligence collection activities;

(2) evaluates the success of the intelligence community in sharing relevant, actionable intelligence with covered entities;

(3) provides an overview of—

(A) intelligence information shared with covered entities pursuant to subsection (c);

(B) notifications withheld pursuant to subsection (c)(3);

(C) outcome of periodic reviews required under subsection (c)(4); and

(4) addresses any legislative or policy changes necessary to enable the intelligence community to increase sharing of actionable intelligence with covered entities.

(h) INTELLIGENCE SHARING.—Notwithstanding any other provision of law, information or intelligence shared with covered entities under the processes established under this section shall not constitute favoring one private entity over another.

SEC. 112 OPERATIONAL COLLABORATION BETWEEN SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE AND THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY AND OTHER RELEVANT FEDERAL AGENCIES.

(a) In General– The head of the office for joint cyber planning established pursuant to Section [xx] of the Homeland Security Act of 2002, in carrying out the responsibilities of such office with respect to relevant cyber defense planning, joint cyber operations, cybersecurity exercises, and information-sharing practices, shall, to the extent practicable, prioritize the involvement of owners and operators of systems, assets, and facilities designated as systemically important critical infrastructure.