.....

(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to designate the Department of Homeland Security as the Sector Risk Management Agency for the information technology sector, require the Cybersecurity and Infrastructure Security Agency to carry out the responsibilities of the Department for such sector, strengthen public and private sector engagement to reduce cybersecurity risks to such sector and secure its systems, assets, and key resources against cybersecurity threats, supply chain compromise, and physical threats, including terrorism threats to the United States, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Homeland Security Act of 2002 to designate the Department of Homeland Security as the Sector Risk Management Agency for the information technology sector, require the Cybersecurity and Infrastructure Security Agency to carry out the responsibilities of the Department for such sector, strengthen public and private sector engagement to reduce cybersecurity risks to such sector and secure its systems, assets, and key resources against cybersecurity threats, supply chain com-

promise, and physical threats, including terrorism threats to the United States, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Sector Engagement for Cybersecurity through Unified Responsibility and Expertise in Information Technology Act'' or the ''SECURE IT Act''.

SEC. 2. INFORMATION TECHNOLOGY SECTOR RISK MANAGEMENT.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by inserting after section 2218 (6 U.S.C. 665d) the following new section:

''SEC. 2218A. INFORMATION TECHNOLOGY SECTOR RISK MANAGEMENT AGENCY.

''(a) DESIGNATION AND ACCOUNTABILITY.—

''(1) DESIGNATION.—The Department shall be the Sector Risk Management Agency for the information technology sector, in accordance with the designation of the Department as the Sector Risk Management Agency for such sector pursuant to National Security Memorandum–22, issued April 30, 2024 (relating to critical infrastructure security and resilience).

''(2) IMPLEMENTATION THROUGH THE AGENCY.—The Secretary, acting through the Director, shall carry out the responsibilities of the Department as the Sector Risk Management Agency for the information technology sector, including the responsibilities described in section 2218 and this section. The Director shall carry out all such responsibilities in a manner that is coordinated with, and supports, the responsibility of the Director under section 2202(c)(4) to coordinate a national effort to secure and protect against critical infrastructure risks and the role of the Agency as the national coordinator for the security and resilience of critical infrastructure pursuant to National Security Memorandum–22, issued April 30, 2024 (relating to critical infrastructure security and resilience).

''(3) ACCOUNTABLE OFFICIAL.—Not later than 90 days after the date of the enactment of this section, the Director shall designate a senior official of the Agency who shall oversee the implementation of this section on behalf of the Director, and who shall serve as the principal point of contact of the Department for the information technology sector. The Director shall provide such official with access to the

personnel and capabilities of the Agency necessary to carry out such implementation.

''(4) SECTOR EXPERTISE AND CONTINUITY.—The Director shall assign personnel to carry out this section who have, or have access to, expertise in the operations of the information technology sector, including expertise relating to data centers, cloud computing, hardware and software supply chains, artificial intelligence, quantum computing, cybersecurity and threat analysis, security testing and adversary emulation (including testing performed with artificial intelligence systems), and physical security. Such personnel shall include analysts who maintain regular engagement with analysts of information technology sector entities and of Information Sharing and Analysis Organizations that serve such sector, and may include personnel who also support other critical infrastructure sectors. The Director shall maintain arrangements to ensure the continuity of such engagement during changes in personnel.

''(5) RELATIONSHIP TO SECTOR DESIGNATION PROCESS.—The process for reviewing critical infrastructure sector designations, subsector designations, and Sector Risk Management Agency designations under section 9002(b) of the William M. (Mac)

Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(b)) shall continue to apply, except that the Department shall remain the Sector Risk Management Agency for the information technology sector pursuant to paragraph (1).

''(b) SCOPE OF THE INFORMATION TECHNOLOGY SECTOR.—

''(1) FUNCTIONS.—In carrying out this section, the Director shall address the security and resilience of the systems and assets, whether physical or virtual, and the key resources of the information technology sector that perform or support the following:

''(A) The design, development, or provision of hardware, firmware, or software, including processors, accelerators, and other computing components, used to create, process, store, secure, or exchange data through information systems.

''(B) The operation of data centers and artificial intelligence compute infrastructure that provide computing, storage, or data processing capacity.

''(C) The provision of products or services by cloud service providers or managed service providers.

''(D) The development, provision, or security of artificial intelligence models and artificial intelligence systems, and of the software and services that support such models and systems.

''(E) The development, provision, or operation of quantum computing systems or services or other emerging computing technologies.

''(F) Identity management, authentication, cryptographic key management, digital certificate services, or other services that establish or verify trust in users, devices, software, or automated processes.

''(G) Cybersecurity products or services, including threat intelligence, incident response, managed security services, and security testing (including penetration testing, red teaming, and adversary evaluation), whether performed by individuals or artificial intelligence systems.

''(H) Software development, maintenance, or distribution, including open-source software, software repositories, build systems, and the mechanisms used to deliver software updates.

''(I) Domain name resolution and other internet infrastructure services that support the

routing and resolution of internet traffic, to the extent such services are specific functions of the information technology sector.

''(J) Such other functions as the Director, in collaboration with the Information Technology Sector Coordinating Council, identifies as critical functions of the information technology sector.

''(2) APPLICATION.—

''(A) IN GENERAL.—The functions described in paragraph (1) do not establish a new critical infrastructure sector or subsector, and do not transfer any system, asset, key resource, or function from another critical infrastructure sector to the information technology sector. The Director shall carry out paragraph (1) without regard to any particular technology, architecture, or deployment model used to perform a function described in such paragraph, and may not treat an entity as part of the information technology sector solely on the basis that such entity uses an information system or artificial intelligence.

''(B) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to deter-

mine whether an entity is subject to any requirement under subtitle D or any other provision of law.

''(3) SHARED RESPONSIBILITIES.—In carrying out engagement and assessments and in providing assistance under this section, the Director shall account for the respective operational control, access, and security responsibilities of facility owners and operators, equipment suppliers, cloud service providers, managed service providers, software developers and maintainers, developers and deployers of artificial intelligence systems, providers of security testing services acting under the authorization of a customer, and customers, including tenants of data centers and customers of cloud services. The Director may not presume that any such entity has access to, control over, or responsibility for all systems, data, or activities within a facility or service.

''(4) DEPENDENCIES ON OTHER SECTORS.—The Director shall address the dependence of the information technology sector on other critical infrastructure sectors, and the dependence of other critical infrastructure sectors on the Information Technology Sector, through the coordination carried out under section 2218(b).

''(c) SECTOR RISK MANAGEMENT FUNCTIONS.—In carrying out the responsibilities of the Department as the Sector Risk Management Agency for the information technology sector under section 2218, the Director shall carry out the following:

''(1) Serve as the day-to-day interface of the Department for the prioritization and coordination of activities relating to the security and resilience of the information technology sector, and as the chair of the Federal Government coordinating council for such sector.

''(2) Offer to information technology sector entities, on a voluntary basis, and giving priority to such entities with limited resources, vulnerability assessments, physical security assessments, architecture reviews, evaluations of security controls, and other technical assistance, prioritized in accordance with subsection (f)(7).

''(3) Facilitate the timely sharing of cyber threat indicators, defensive measures, and information relating to cybersecurity threats and physical threats among the Agency, information technology sector entities, and the Homeland Security Enterprise, including through Information Sharing and Analysis Organizations, the national cybersecurity

and communications integration center established under section 2209, and the office established under section 2216.

''(4) Identify, in consultation with information technology sector entities, the threat information needs and priorities of such entities and of the information technology sector as a whole, and provide threat information responsive to such needs and priorities that includes practical mitigations and, where available, the level of confidence in and the limitations of the underlying analysis, at the lowest classification level consistent with the protection of sources and methods.

''(5) Make available and routinely review the process of application for security clearances under section 2212 to appropriate representatives of information technology sector entities, and facilitate access to classified threat briefings by appropriately cleared representatives of such entities.

''(6) Support incident management, restoration, and national cybersecurity asset response activities affecting the information technology sector, including activities carried out under subtitle C with respect to a significant incident declared under section 2233, and coordinate with affected information tech-

nology sector entities and the customers of such entities in carrying out such activities, without displacing the operational control of any such entity or customer over its own systems and assets.

''(7) Conduct, or facilitate the participation of information technology sector entities in voluntary exercises, including under the National Cyber Exercise Program established under section 2220B, that address the disruption and recovery of products, services, and providers on which multiple critical infrastructure sectors depend, and use the lessons learned from such exercises to improve assistance and planning under this section.

''(8) Support resilience, continuity and recovery planning, including through the promotion of voluntary preparedness standards, that accounts for dependencies among facilities, services, and providers, including restoration sequencing, the availability of backup and replacement capabilities, and the risk that services that appear to be redundant depend on the same underlying systems.

''(9) Collaborate with information technology sector entities to prioritize the use of the limited resources of the Agency and of such entities to ad-

dress the risks that present the greatest potential consequences to the following:

''(A) The information technology sector.

''(B) Critical infrastructure sectors that depend on the information technology sector.

''(10) Promote the use by information technology sector entities of existing voluntary consensus standards, security practices (including practices for continuous security validation and testing), and guidance, and work to reduce duplicative or conflicting security recommendations applicable to such entities.

''(11) Coordinate, as appropriate, with SLTT entities and emergency response providers, including through Cybersecurity State Coordinators appointed under section 2217, regarding emergency preparedness, physical security, incident response, and recovery affecting systems and assets of the information technology sector located within the jurisdictions of such SLTT entities.

''(d) PARTNERSHIP WITH THE INFORMATION TECHNOLOGY SECTOR.—

''(1) SECTOR COORDINATING COUNCIL.—The Director shall collaborate with the Information Technology Sector Coordinating Council as the pri-

vate sector counterpart of the Department for the information technology sector in identifying priorities and developing, implementing, and evaluating activities under this section. Nothing in this subsection may be construed to authorize the Director to direct or control the organization, membership, or governance of such Council or of any Information Sharing and Analysis Organization.

''(2) BROAD PARTICIPATION.—The Director shall seek input from information technology sector entities of different sizes, business models, and technical capabilities, as relevant to each activity under this section, including from small and midsize entities, owners and operators of data centers, cloud service providers, providers of hardware and software, developers of artificial intelligence and quantum computing technologies, maintainers of open source software, providers of security testing services (including penetration testing, red teaming, and adversary emulation services), and security researchers. Membership of any such entity in any particular council or organization shall not be a condition of receiving assistance or information under this subsection.

''(3) USE OF EXISTING MECHANISMS.—The Secretary and the Director shall, to the maximum extent practicable, carry out this section through existing sector and cross-sector partnerships, government coordinating councils, and advisory mechanisms, including any framework of advisory committees established pursuant to section 871. Nothing in this subsection requires the establishment of a new partnership, council, committee, task force, working group, or other advisory mechanism, and the establishment of any such partnership, council, committee, task force, working group, or other advisory mechanism, as the case may be, shall not be a prerequisite to engagement under this subsection.

''(4) FEDERAL GOVERNMENT COORDINATING COUNCIL.—The Federal Government coordinating council chair for the information technology sector pursuant to section 2218(c)(3)(B) shall be composed of representatives of executive agencies with responsibilities relating to the security and resilience of the information technology sector, and may include representatives of SLTT entities.

''(5) PARTNERSHIP PRINCIPLES.—In carrying out this section, the Director shall, to the maximum extent practicable, carry out the following:

''(A) Provide timely, actionable, and bidirectional sharing of information with information technology sector entities.

''(B) Provide the Information Technology Sector Coordinating Council and other relevant information technology sector entities a reasonable opportunity to help identify the objectives and practical requirements of a sector-specific risk management plan or voluntary guidance under this section before such plan or guidance, as the case may be, is developed, and to review such draft before issuance, and communicate how significant technical concerns raised by such entities were addressed.

''(C) Provide an identifiable point of contact within the Agency for assistance under this section, consolidate requests for information directed to information technology sector entities across components of the Department, and use information previously provided to the Department when such information is lawfully available, sufficiently current, and used consistent with any restrictions that apply to such information.

''(D) During an incident, lead coordination with other components of the Department and with other executive agencies to carry out the following:

''(i) Reduce duplicative requests to information technology sector entities affected by such incident and to the customers of such entities.

''(ii) Avoid conflicting operational communications and outreach.

''(E) Account for the resources, capabilities, and operational demands of information technology sector entities, including small and midsize entities and maintainers of open-source software with limited resources.

''(F) Recognize and leverage the security investments, capabilities, and expertise of information technology sector entities, including the capabilities of such entities to carry out the following:

''(i) Detect and respond to cybersecurity threats.

''(ii) Identify and validate exploitable security vulnerabilities, at scale, including through the use of artificial intelligence.

"(6) RULE OF APPLICATION.—Paragraph (5)(B) shall not require the disclosure of protected information or delay any warning, response, or other action necessary to address a time sensitive threat, security vulnerability, or disruption.

"(e) INFORMATION SHARING AND VULNERABILITY COORDINATION.—

"(1) ANALYTIC COLLABORATION.—The Director shall maintain a capability, using existing systems and partnerships, including the Agency's Threat Intelligence Enterprise Services program or successor program, to the maximum extent practicable, through which participating information technology sector entities and Information Sharing and Analysis Organizations may exchange timely threat information with analysts of the Agency, identify shared analytic priorities, and receive analysis and mitigation information responsive to such priorities in near real time where practicable. Such capability—

"(A) shall—

"(i) support automated exchange where useful and practicable;

"(ii) support bidirectional information sharing and operational collaboration; and

''(iii) be designed to be interoperable with the processes of the Agency for receiving, analyzing, and sharing information under subtitle D; and

''(B) may not require the use of a particular platform or continuous access to the information systems of any participant.

''(2) VOLUNTARY SHARING AND FEEDBACK.—

''(A) IN GENERAL.—The Director shall carry out the following:

''(i) Facilitate the use of existing channels for the voluntary sharing of information relating to incidents, attempted intrusions, supply chain compromises, security vulnerabilities, insider threat activities, and other activities relevant to cybersecurity risks or physical threats, including activities that did not result in a compromise of an information system.

''(ii) Inform entities that share information under subparagraph (A) of the handling procedures and protections that apply to such information.

''(iii) To the extent practicable, provide such entities with analysis derived

from such information and feedback on how such information was used.

''(B) PROHIBITION.—The Directory may not disseminate information relating to the system of a customer of an information technology sector entity that is derived from security testing performed for such customer if such information is in a form that identifies, or could reasonably be used to identify, such customer, except with the consent of such customer or as otherwise required by law.

''(3) VULNERABILITY COORDINATION AND COMPENSATING CONTROLS.—The Director, in consultation with the Director of the National Institute of Standards and Technology and existing vulnerability coordination initiatives, shall, in collaboration with relevant developers, providers, maintainers, security researchers, trusted cybersecurity partners, providers of security testing services, providers of vulnerability management services, and other appropriate participants, improve the coordinated vulnerability disclosure processes of the Agency to address increases in the speed and volume of the discovery and exploitation of security vulnerabilities, including through the use of artificial intelligence, and develop

a secure mechanism for sharing vulnerability information among trusted cybersecurity partners prior to vulnerability disclosure, for the purpose of developing and deploying compensating controls such as advanced virtual patching. Such improvements and mechanism shall account for the following:

''(A) Verification, reproducibility, duplicate reports, and prioritization based on exploitation, exposure, and potential consequences using standardized, machine-readable vulnerability schemas.

''(B) Secure coordination among relevant providers, trusted cybersecurity partners, and their downstream customers and users, including maintainers of open-source software with limited resources.

''(C) The time and testing necessary to develop, validate, and safely deploy mitigations, including the following:

''(i) Staged deployment.

''(ii) The ability to reverse a defective update.

''(iii) Compensating controls, such as advanced virtual patching, when a patch is not yet available.

''(D) The respective roles of automated vulnerability discovery and remediation tools and human judgment, and the risks of disclosing actionable exploitation details before effective mitigations are reasonably available, and whether certain details should remain withheld after such mitigations are available.

''(E) Secure, standardized protocols and operational safeguards for the timely sharing of vulnerability data with trusted cybersecurity partners solely to facilitate the joint development, validation, and distribution of dynamic virtual patches and other compensating controls that provide protection against adversary exploitation prior to vendor patch release.

''(F) Combinations of security vulnerabilities, within or across products or projects, that together enable exploitation, including coordination of such combinations among multiple relevant parties, and prioritization based on the resulting potential consequences rather than the severity of each individual security vulnerability.

''(G) Validation, through testing where practicable, that a mitigation prevents the ex-

ploitation it is intended to address, and communication of whether a version of a product has been assessed, so that the absence of a reported security vulnerability is not presumed to indicate the absence of risk.

''(H) Security vulnerabilities that have been remediated without public notice or an identifier and that remain present in versions of products still in use, other than security vulnerabilities in services for which the provider has applied the remediation without requiring action by customers.

''(I) The use of existing vulnerability identifiers, machine-readable formats, and coordination programs, including industry-led and nonprofit programs, without establishing a duplicative identification scheme.

''(J) Protections for the identity of reporters and for confidential information of the customers in whose environments a security vulnerability was identified

''(K) Mechanisms to protect good-faith security researchers and independent artificial intelligence safety evaluators engaged in coordinated vulnerability testing, red-teaming, or

model robustness evaluations conducted in accordance with established voluntary disclosure policies from civil or criminal liability.

''(4) RELATIONSHIP TO CYBER INCIDENT REPORTING.—Voluntary sharing under this subsection does not satisfy or alter any reporting obligation under subtitle D or any other provision of law, except to the extent provided by such law. Information obtained under subtitle D may be used to carry out this section only in accordance with the purposes, protections, and restrictions of such subtitle.

''(f) SECTOR-SPECIFIC RISK MANAGEMENT PLAN AND RISK ASSESSMENT.—

''(1) INITIAL PLAN AND ASSESSMENT.—Not later than 18 months after the date of the enactment of this section, the Director, in collaboration with the Information Technology Sector Coordinating Council, shall develop a sector-specific risk assessment for the information technology sector and a sector-specific risk management plan for such sector that is informed by such assessment. Such assessment may be included as an annex to such plan.

''(2) RECURRING UPDATES.—Not less frequently than once every two years after the development of the assessment and plan under paragraph

(1), the Director shall review and update such assessment and plan in accordance with such paragraph. An update may incorporate by reference material that remains current, and shall identify material changes in risks, priorities, or planned activities or progress made in implementing the immediately preceding plan. The Director shall provide targeted updates between such reviews when a material change in risk warrants such an update.

''(3) ASSESSMENT METHOD.—Each assessment under this subsection shall identify and prioritize the most significant risks to the security or resilience of the information technology sector and its critical functions, based on threats and hazards, security vulnerabilities, the likelihood and consequences of disruption or compromise, and existing mitigations. In conducting each such assessment, the Director shall carry out the following:

''(A) Assess risk primarily to the critical functions of the information technology sector referred to in subsection (b)(1), and any other functions determined necessary by the Director and the Information Technology Sector Coordinating Council, consistent with the functions-based approach to risk assessment previously

developed by the Department and the Information Technology Sector Coordinating Council, rather than relying primarily on inventories of individual systems and assets.

''(B) Distinguish observed conditions from projections, and identify material uncertainties, data limitations, and assumptions, without requiring a numerical estimate when reliable information is not available.

''(C) Consider the duration and geographic reach of potential disruptions, recovery capabilities, interdependencies, and consequences for national security, national economic security, and national public health or safety.

''(D) Use relevant information lawfully available to the Director, including existing assessments, threat intelligence, voluntarily shared information, and information available under subtitle D subject to subsection (e)(4), without requiring any entity to prepare a separate assessment or to submit information under this section.

''(4) RISK CONSIDERATIONS.—Each assessment under this subsection shall consider, to the extent

relevant to the most significant risks to the information technology sector, the following:

''(A) Malicious activity by covered foreign adversaries, including efforts to gain or maintain access to systems and assets of the information technology sector for the purpose of future disruption or destruction, the use of compromised systems and assets of such sector, including virtual infrastructure and network devices, for malicious cyber command and control or malicious reconnaissance, and efforts to steal intellectual property, sensitive data, and model weights.

''(B) Terrorism threats to the United States involving the targeting or disruption of systems and assets of the information technology sector, including the threat of physical attack against data centers and supporting infrastructure by terrorist organizations, covered foreign adversaries, or individuals acting alone, including attacks carried out through the use of unmanned aircraft systems.

''(C) Ransomware attacks and other criminal threats to information technology sector en-

tities and to the customers that depend on such entities.

''(D) Insider threats, including the use of fraudulent or deceptive employment or contracting practices by individuals acting on behalf of covered foreign adversaries to obtain access to information technology sector entities, and including insider threats posed by artificial intelligence agents.

''(E) Supply chain compromise affecting hardware, firmware, software, or services, including development, build, or update mechanisms, open-source software, or components sourced from covered foreign countries.

''(F) Cybersecurity risks to artificial intelligence systems or the environments in which such systems are developed or operated, including unauthorized access to or alteration of model weights, training and evaluation data, credentials, or associated software, and actions taken by such systems beyond their authorized access or intended operational boundaries.

''(G) The use of artificial intelligence by threat actors to discover and exploit security vulnerabilities at scale, in order to—

''(i) inform opportunities to use artificial intelligence to identify and validate such exploitable security vulnerabilities before such vulnerabilities are so exploited; and

''(ii) improve detection, mitigation, and recovery related to such use.

''(H) Physical security risks or cybersecurity risks to data centers, including risks to industrial control systems, physical access control systems, power distribution, cooling, fire suppression, or remote maintenance systems, and relevant natural and physical hazards, including an EMP or a GMD.

''(I) Shared dependencies and common causes of failure among products, services, administrative systems, and providers, including disruptions not caused by malicious activity and cascading consequences for customers and other critical infrastructure sectors.

''(J) Dependencies of the information technology sector on energy, communications, water, transportation, or other services, including, to the extent practicable, dependencies on

infrastructure located outside the United States.

''(K) Risks to quantum computing systems or services, and risks to cryptographic protections from advances in quantum computing, including the collection of encrypted data for later decryption, the period for which such data requires protection, and the time required to transition dependent systems to new cryptographic mechanisms.

''(L) Risks to the security or resilience of internet infrastructure and domain name systems, including risks arising when multiple mission-critical operational, identity, management, or trust functions depend on a common point of failure, compromise, or administrative control that is not mitigated by security controls, redundancy, or recovery capabilities.

''(M) Emerging technologies and changes in the architecture and operating models of the information technology sector that are reasonably likely to materially affect the security or resilience of such sector during the period of five years beginning on the date of such assessment.

''(5) PLAN CONTENTS.—Each plan under this subsection shall include the following:

''(A) The prioritized activities the Department will carry out to address the most significant risks identified in the most recent assessment, the officials responsible for such activities, milestones, and the personnel and resources available or needed to carry out such activities.

''(B) A description of the information sharing, analytic collaboration, technical assistance, incident response, recovery, and exercise activities the Department will carry out under this section.

''(C) The approach of the Department to addressing dependencies between the information technology sector and other critical infrastructure sectors, and to coordinating assistance to entities that perform functions in more than one such sector.

''(D) Activities to address risks to data centers, artificial intelligence compute infrastructure, artificial intelligence systems, hardware or software supply chains, internet infrastructure, or quantum computing or other

emerging computing technologies, as warranted by the most recent assessment.

''(E) A description of the existing voluntary consensus standards, security practices, or guidance the Department will promote, including efforts to identify gaps and avoid duplicative or conflicting recommendations.

''(F) Objective measures of the effectiveness of the activities of the Department under this section, including the timeliness and usefulness of information or assistance, progress in addressing identified risks and exercise findings, and voluntary feedback from information technology sector entities, rather than reliance solely on the number of meetings held, participants engaged, or products issued.

''(G) Steps to make information and assistance under this section accessible to small and midsize entities and entities that do not participate in established partnership structures.

''(H) For each plan after the initial plan, a description of progress made in implementing the preceding plan, and an explanation of any material delay, unaddressed priority, or gap in

the authorities, capabilities, or resources of the Department.

''(6) ALIGNMENT AND CONSOLIDATION.—The Director shall align each assessment and plan under this subsection with national critical infrastructure risk management planning, including planning under National Security Memorandum–22, issued April 30, 2024 (relating to critical infrastructure security and resilience), or any successor document. An existing assessment or plan may satisfy the requirements of this subsection, if the Director supplements such assessment or plan, as the case may be, to the extent necessary to satisfy such requirements. The Director may make a one-time adjustment of not more than six months to the schedule under paragraph (2) to align such schedule with a national planning cycle, after providing notice to the appropriate congressional committees that explains such adjustment.

''(7) PRIORITIZATION OF ASSISTANCE.—The Director shall use each assessment and plan under this subsection to prioritize voluntary assistance based on potential consequences, dependencies, existing mitigations, or the need for Federal support, including among information technology sector entities with limited resources. The Director may use exist-

ing processes for identifying significant systems and assets, as appropriate, but may not establish under this section any regulatory designation, public ranking, or mandatory inventory of information technology sector entities or of the systems and assets of such entities.

''(g) DATA CENTER AND COMPUTE INFRASTRUCTURE SECURITY.—

''(1) VOLUNTARY ASSISTANCE AND GUIDANCE.—Based on the most recent assessment and plan under subsection (f), the Director shall develop, adapt, or make available voluntary assistance and guidance, in consultation with owners and operators of data centers and artificial intelligence compute infrastructure, that addresses physical security risks or cybersecurity risks during the planning, design, construction, operation, maintenance, or decommissioning of data centers or artificial intelligence compute infrastructure, including relating to the following:

''(A) The security of facility control systems, remote administration, privileged access, and third party maintenance.

''(B) The isolation of customers and workloads, the protection of sensitive information,

and the security of shared computing and management capabilities, consistent with the shared responsibilities described in subsection (b)(3).

''(C) The protection of model weights and other sensitive data against unauthorized access, theft, or exfiltration.

''(D) The resilience of supporting systems, and practical approaches to continued operation, safe shutdown, and recovery.

''(E) Opportunities to address security risks during design and construction, without making consultation with, or approval by, the Agency a condition of the siting, construction, or operation of any facility.

''(2) THREAT BRIEFINGS.—The Director shall provide threat briefings, including classified briefings for appropriately cleared personnel, to owners and operators of data centers and artificial intelligence compute infrastructure regarding cybersecurity threats and physical threats, including terrorism threats to the United States and threats posed by covered foreign adversaries.

''(3) EXISTING VOLUNTARY PROGRAMS.—The Director shall facilitate access by eligible owners and operators of data centers and artificial intelligence

compute infrastructure to relevant voluntary programs of the Agency, including the CyberSentry program established under section 2220C, consistent with the eligibility criteria, consent requirements, and availability of resources applicable to each such program.

''(h) ARTIFICIAL INTELLIGENCE SECURITY ASSISTANCE.—The Director, in consultation with the Director of the National Institute of Standards and Technology, in accordance with existing Federal voluntary frameworks, and in alignment with industry-standard artificial intelligence safety frameworks, shall develop, adapt, or make available voluntary assistance and guidance, in consultation with cybersecurity providers and developers, and developers and deployers of artificial intelligence systems, that addresses cybersecurity risks to artificial intelligence systems, their components, or the environments in which such systems are developed or operated, including relating to the following:

''(1) The unauthorized acquisition, alteration, or disclosure of model weights, proprietary training data, source code, or other sensitive information.

''(2) The integrity of data, software dependencies, artificial intelligence models, or updates obtained from third parties.

''(3) Access controls, credentials, isolation, or least-privilege execution environments or monitoring appropriate to artificial intelligence systems that are capable of taking actions within or through other information systems.

''(4) The detection, containment, or recovery of artificial intelligence systems that exceed their authorized access or intended operational boundaries.

''(5) Differences among development or deployment arrangements, including artificial intelligence models with publicly available model weights, except that the authorized release or use of publicly available model weights shall not be treated as an incident solely on such basis.

''(6) Practices for authorizing, scoping, logging, or constraining artificial intelligence systems used to conduct authorized security testing, including written rules of engagement, mechanisms to halt such systems, and audit records.

''(i) SUPPLY CHAIN SECURITY.—The Director shall support voluntary collaboration among information technology sector entities relating to the risk of supply chain compromise through existing partnerships, including existing mechanisms that address risks affecting multiple crit-

ical infrastructure sectors. Such collaboration shall address the following:

''(1) The integrity and provenance of hardware, firmware, software, and updates, including risks associated with components sourced from covered foreign countries and the risk that components from trusted sources are compromised.

''(2) Risks associated with access to or control over products, services, or suppliers by covered foreign adversaries.

''(3) Dependencies on components or suppliers for which limited alternatives exist.

''(4) The practical costs, lead times, support requirements, and operational consequences of mitigation measures.

''(j) CRYPTOGRAPHIC UPGRADE AND QUANTUM READINESS.—The Director shall facilitate access by information technology sector entities to existing standards and guidance, and shall offer voluntary assistance, relating to the identification of cryptographic dependencies, the prioritization of migration, interoperability testing, and the ability to replace or adapt cryptographic mechanisms while maintaining security and operations, including the upgrade to cryptographic algorithms that are resistant to attack by quantum computers. Activities under this sub-

section shall account for product support periods, supplier readiness, and risks to availability, and may not establish a mandatory migration schedule or a separate cryptographic standard.

''(k) PRACTICAL IMPLEMENTATION.—In carrying out this section, the Director shall account for differences in the size, technical capabilities, operating environments, or resources of information technology sector entities, the respective responsibilities of suppliers and customers, and the need to validate changes and avoid unnecessary interruption of essential services. Assistance and guidance under this section may not presume that the use of multiple providers, the relocation of workloads, or the replacement of an integrated platform is necessary or feasible in every case.

''(l) VOLUNTARY PARTICIPATION AND PROTECTION OF INFORMATION.—

''(1) VOLUNTARY PARTICIPATION.—Participation by any non-Federal entity in an activity under this section shall be voluntary. The Director may not—

''(A) condition assistance under this section on the disclosure of information unrelated to the assistance requested;

''(B) treat a decision to not so participate as evidence of deficient security or of non-compliance with law; or

''(C) require, request, or condition assistance upon the submission, transfer, or custody of artificial intelligence model weights, model parameters, or proprietary source code.

''(2) ACCESS AND CONSENT.—Any access to, or monitoring of, an information system of a non-Federal entity to provide assistance under this section shall be subject to the express consent of an entity authorized to provide such consent and a written agreement that identifies the scope and purposes of such access or monitoring, as the case may be, the handling of information, and the means of ending such access or monitoring, as the case may be. Consent provided by an entity under this paragraph does not authorize access to the systems or information of a customer of such entity beyond the lawful authority of such entity.

''(3) EXISTING INFORMATION PROTECTIONS.—An entity may submit information in connection with an activity under this section as critical infrastructure information under subtitle B when the conditions of such subtitle are satisfied, and infor-

mation so submitted shall receive the protections provided under section 2224. Information shared pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) shall be handled in accordance with such Act. This section does not expand the categories of information protected under such subtitle or such Act, as the case may be, or waive any condition for receiving such protections.

''(4) HANDLING SAFEGUARDS.—The Director shall maintain procedures for information obtained under this section that carry out the following:

''(A) Limit the collection and use of such information to information reasonably necessary to carry out this section or for a cybersecurity purpose, and use aggregated or otherwise less sensitive information when adequate.

''(B) Protect critical infrastructure information, trade secrets, proprietary information, personal information, artificial intelligence model weights, evaluation datasets, benchmark results, security or technical metadata relating to artificial intelligence model weights, and other sensitive information against unauthorized access, use, retention, or disclosure, consistent with applicable law, and ensure that any

such information, trade secrets, proprietary information, personal information, artificial intelligence model weights, evaluation datasets, benchmark results, security or technical metadata relating to artificial intelligence model weights, or other sensitive information provided voluntarily to the Department shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act').

''(C) Apply access controls, retention schedules, and restrictions on further dissemination appropriate to such information, and preserve the protections and restrictions that apply under the authority through which such information was obtained.

''(D) Provide for the dissemination of analysis in a form that does not identify a submitting entity or expose its confidential information, except with the authorization of such entity or as otherwise required or authorized by law.

''(5) PRIVACY AND CIVIL LIBERTIES.—The Director shall carry out this section in consultation with the senior official appointed under section 222

and the Officer for Civil Rights and Civil Liberties of the Department.

''(m) OVERSIGHT AND TRANSPARENCY.—

''(1) IMPLEMENTATION BRIEFING.—Not later than 180 days after the date of the enactment of this section, the Director shall brief the appropriate congressional committees on the designation of the official under subsection (a)(3), the partnerships under subsection (d), and the milestones and resources necessary to implement this section.

''(2) SUBMISSION OF PLANS AND ASSESSMENTS.—Not later than 30 days after completing or updating an assessment and plan under subsection (f), the Director shall submit such assessment and plan to the appropriate congressional committees. Each such assessment and plan shall be submitted in unclassified form to the extent practicable, but may include a classified annex.

''(3) SECTOR AND PUBLIC INFORMATION.—The Director shall publish a summary of each plan and update under subsection (f) that describes priorities, planned activities, progress, and how to obtain assistance, and shall make additional actionable information available to information technology sector entities consistent with applicable protections. Each

such summary may not disclose security vulnerabilities, sensitive dependencies, or confidential information of any specific information technology sector entity.

''(4) QUARTERLY BRIEFINGS.—

''(A) IN GENERAL.—Not later than 30 days after the briefing under paragraph (1) and not less frequently than once every 90 days thereafter, the Director shall brief the appropriate congressional committees on cybersecurity risks, cybersecurity threats, or physical threats to the information technology sector, including terrorism threats to the United States, and on the activities of the Department under this section.

''(B) CONTENTS.—Each briefing under subparagraph (A) shall include information relating to the following:

''(i) Each significant incident, ransomware attack, or supply chain compromise affecting information technology sector entities, or affecting other critical infrastructure sectors through the products or services of such entities, that occurred or was identified since the immediately

preceding briefing, and the actions taken by the Department in response, including national cybersecurity asset response activities. The Director shall describe each such incident, attack, or compromise in a manner that does not identify an affected entity the involvement of which has not been publicly disclosed, unless any appropriate congressional committee requests such identification.

''(ii) Significant cybersecurity threats or physical threats to the information technology sector, including threats posed by covered foreign adversaries and terrorism threats to the United States involving data centers or artificial intelligence compute infrastructure.

''(iii) Security vulnerabilities in products or services of the information technology sector that are known to be actively exploited, and the status of coordinated vulnerability disclosure and mitigation efforts relating to such vulnerabilities.

''(iv) The threat information, cyber threat indicators, defensive measures, or

other products shared with information technology sector entities since the immediately preceding briefing, and the timeliness of such sharing.

''(v) Engagement with the Information Technology Sector Coordinating Council, Information Sharing and Analysis Organizations, and SLTT entities, including any significant concern raised by such entities and the response of the Department.

''(vi) Progress in implementing the most recent plan under subsection (f), the personnel, expertise, and resources assigned to carry out this section, and any vacancy or resource shortfall that affects such implementation.

''(vii) Voluntary feedback from information technology sector entities regarding the timeliness and usefulness of information and assistance provided under this section.

''(C) ANNUAL RECOMMENDATIONS.—Not less frequently than once each year, a briefing under subparagraph (A) shall include any recommendation of the Director for legislative or

administrative action to improve the security or resilience of the information technology sector.

"(D) FORM.—

"(i) IN GENERAL.—Each briefing under subparagraph (A) shall be provided in a classified setting and may include an unclassified session. The Director may provide such a briefing jointly or separately to each of the appropriate congressional committees, and may combine such a briefing with any other briefing to the appropriate congressional committees that addresses the matters described in subparagraph (B), subject to the approval of the Chairman of such committee.

"(ii) REQUIREMENTS.—In providing a briefing under subparagraph (A), the Director—

"(I) shall—

"(aa) protect the identity and confidential information of any information technology sector entity that voluntarily shared information under this section, un-

less such entity expressly consents to disclosure; and

''(bb) provide any named or identifiable information technology sector entity a reasonable opportunity to verify the technical accuracy of information relating to its products or services prior to such a briefing; and

''(iii) may not disclose actionable exploitation details or unmitigated security vulnerabilities in any unclassified session.

''(5) BUDGET DISPLAY.—The Secretary shall include in the budget justification materials submitted to Congress in support of the budget of the Department for each fiscal year an identification of the amounts and full-time equivalent positions requested to carry out this section. Resources shared with other functions of the Agency may be described through reasonable estimates, together with an explanation of the method of allocation.

''(n) NATIONAL SECURITY SYSTEMS.—Nothing in this section applies to a national security system.

''(o) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate.

''(2) ARTIFICIAL INTELLIGENCE.—The term 'artificial intelligence' has the meaning given such term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

''(3) ARTIFICIAL INTELLIGENCE AGENT.—

''(A) IN GENERAL.—The term 'artificial intelligence agent' means a software system that—

''(i) uses artificial intelligence to plan, select, or sequence actions toward an objective assigned by a user, organization, or other system;

''(ii) has been granted access, credentials, or permissions that enable such agent to carry out such actions within or through an information system, including by invoking tools, calling application programming interfaces, operating a software user inter-

face, accessing or modifying data, or directing other software; and

''(iii) can carry out such actions without requiring human approval of each such action; and

''(B) EXCLUSION.—The term 'artificial intelligence agent' does not include—

''(i) software that executes only predetermined instructions without the use of artificial intelligence to determine the actions of such agent; or

''(ii) an artificial intelligence system that only generates content, recommendations, or analysis for review by a human user and cannot itself take action within or through an information system.

''(4) ARTIFICIAL INTELLIGENCE COMPUTE INFRASTRUCTURE.—The term 'artificial intelligence compute infrastructure' means processors, accelerators, and other specialized computing hardware, together with the associated networking, storage, power distribution, cooling, and control systems, that are used at scale to train, evaluate, or operate artificial intelligence models.

''(5) ARTIFICIAL INTELLIGENCE MODEL.—The term 'artificial intelligence model' means a component of an artificial intelligence system that is derived using mathematical, computational, statistical, or machine learning techniques and that is used to produce outputs from a given set of inputs.

''(6) ARTIFICIAL INTELLIGENCE SYSTEM.—The term 'artificial intelligence system' means any of the following:

''(A) Artificial intelligence.

''(B) A system, software, hardware, model, tool, or other utility that operates in whole or in part through the utilization of artificial intelligence.

''(7) ASSETS.—The term 'assets' means a person, structure, facility, information, material, equipment, network, or process, whether physical or virtual, that enables an organization's services, functions, or capabilities.

''(8) COVERED FOREIGN ADVERSARY.—The term 'covered foreign adversary' means—

''(A) any foreign government, military, intelligence service, or other authority of a covered foreign country acting independently; or

''(B) any organization, group, or person acting on behalf of, with the support, direction, control, or influence of, or trained or supplied by, such a foreign government, military, intelligence service, or other authority, as the case may be, including any proxy, militia, paramilitary organization, intelligence or security service, or other state-sponsored actor that receives material support, training, technical assistance, or operational coordination from a covered foreign country and engages in activities that threaten the national security of the United States or its allies.

''(9) COVERED FOREIGN COUNTRY.—The term 'covered foreign country' means a country that—

''(A) the intelligence community has identified as a foreign adversary in its most recent Annual Threat Assessment; or

''(B) the Secretary, in coordination with the Director of National Intelligence, has identified as a foreign adversary that is not included in such Annual Threat Assessment.

''(10) DATA CENTER.—The term 'data center' means a facility, a group of interconnected facilities, or a portion of a facility, that is primarily used to

house and operate information systems that provide computing, storage, or data processing capacity, including a facility that provides co-location services, together with the industrial control systems, physical security systems, power distribution and cooling systems, and other supporting systems of such facility to the extent such systems are under the operational control of the owner or operator of such facility. Such term does not include a communications network, an electric utility system, or other internal or external infrastructure solely because such network, system, or infrastructure serves such a facility.

''(11) INFORMATION TECHNOLOGY SECTOR.—The term 'information technology sector' means the critical infrastructure sector identified as the Information Technology Sector in National Security Memorandum–22, issued April 30, 2024 (relating to critical infrastructure security and resilience), or any successor document, and includes the systems, assets, key resources, and functions described in subsection (b).

''(12) INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL.—The term 'Information Technology Sector Coordinating Council' means the council, or any successor council, that is self-orga-

nized and self-governed by owners and operators within the information technology sector, their trade associations, and other industry representatives, and that serves as the sector coordinating council for the information technology sector.

''(13) INFORMATION TECHNOLOGY SECTOR ENTITY.—The term 'information technology sector entity' means an owner or operator of systems or assets within the information technology sector, or a provider of products, services, or functions described in subsection (b)(1).

''(14) MODEL WEIGHTS.—The term 'model weights' means the numerical parameters, including biases and other learned parameters, of an artificial intelligence model that are derived through training and that, in combination with the architecture of such model, are sufficient to enable the functioning of such model.

''(15) SIGNIFICANT INCIDENT.—The term 'significant incident' has the meaning given such term in section 2232.

''(16) SYSTEMS.—The term 'systems' means a combination of personnel, structures, facilities, information, materials, equipment, networks, or processes, whether physical or virtual, integrated or

interconnected for a specific purpose that enables an organization's services, functions, or capabilities.

''(17) TERRORIST ORGANIZATION.—The term 'terrorist organization' means—

''(A) any entity designated as a foreign terrorist organization pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189); or

''(B) any entity engaged in terrorism.

''(18) UNMANNED AIRCRAFT SYSTEM.—The term 'unmanned aircraft system' has the meaning given such term in section 44801 of title 49, United States Code.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 2218 the following new item:

''Sec. 2218A. Information technology sector risk management agency.''.