Amendment to H.R. 2795

AMENDMENT TO H.R. 2795

OFFERED BY MR. SWALWELL OF CALIFORNIA

Page 3, line 9, strike "(F)" and insert "(H)".

Page 3, beginning line 9, insert the following:

"(F) The Office for Civil Rights and Civil Liberties.

"(G) The Privacy Office.".

Page 3, after line 10, insert the following:

"(2) CHARTER.—The Secretary is authorized to issue a charter for the Board, and such charter shall specify the following:

"(A) The Board's mission, goals, and scope of its activities.

"(B) The duties of the Board's representatives.

"(C) The frequency of the Board's meetings.".

Page 3, line 11, strike "(2)" and insert "(3)".

Page 4, line 1, strike "(3)" and insert "(4)".

☒

Amendment in the Nature of a Substitute to H.R. 2980

AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 2980 OFFERED BY MS. JACKSON LEE OF TEXAS

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Vulnerability Remediation Act''.

SEC. 2. CYBERSECURITY VULNERABILITIES.

Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''and'' after the semicolon at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following new paragraph:

''(6) the term 'cybersecurity vulnerability' has the meaning given the term 'security vulnerability' in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and''.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting after subparagraph (A) the following new subparagraph:

''(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and''; and

(iv) in subparagraph (C), as so redesignated, by inserting ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)'' before ''with Federal'';

(B) in paragraph (7)(C), by striking ''sharing'' and inserting ''share''; and

(C) in paragraph (9), by inserting ''mitigation protocols to counter cybersecurity vulnerabilities,'' after ''measures,'';

(3) in subsection (e)(1)(G), by striking the semicolon after ''and'' at the end;

(4) by redesignating subsection (o) as subsection (p); and

(5) by inserting after subsection (n) following new subsection:

''(o) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.''.

SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (n) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (o) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity

vulnerabilities to information systems and industrial control systems, that includes the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (n) and (o) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders.

(4) Any available information on the degree to which such information was acted upon by industry and other stakeholders.

(5) A description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

(b) FORM.—The report required under subsection (b) shall be submitted in unclassified form but may contain a classified annex.

SEC. 4. COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES.

The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 2) to information systems (as such term is defined in such section 2209) and industrial control systems, including supervisory control and data acquisition systems.

SEC. 5. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

(1) HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

"SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.";

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

"SEC. 2216. JOINT CYBER PLANNING OFFICE.";

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";

(D) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".

(2) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint cyber planning office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.''.

Amendment in the Nature of a Substitute to H.R. 3138

AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 3138 OFFERED BY MS. CLARKE OF NEW YORK

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''State and Local Cybersecurity Improvement Act''.

SEC. 2. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

(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 adding at the end the following new sections:

''SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

''(a) DEFINITIONS.—In this section:

''(1) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(2) CYBERSECURITY PLAN.—The term 'Cybersecurity Plan' means a plan submitted by an eligible entity under subsection (e)(1).

''(3) ELIGIBLE ENTITY.—The term 'eligible entity' means—

''(A) a State; or

''(B) an Indian tribe that, not later than 120 days after the date of the enactment of this section or not later than 120 days before the start of any fiscal year in which a grant under this section is awarded—

''(i) notifies the Secretary that the Indian tribe intends to develop a Cybersecurity Plan; and

''(ii) agrees to forfeit any distribution under subsection (n)(2).

''(4) INCIDENT.—The term 'incident' has the meaning given the term in section 2209.

''(5) INDIAN TRIBE; TRIBAL ORGANIZATION.—The term 'Indian tribe' or 'Tribal organization' has the meaning given that term in section 4(e) of the of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e)).

''(6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'information sharing and

analysis organization' has the meaning given the term in section 2222.

''(7) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(8) ONLINE SERVICE.—The term 'online service' means any internet-facing service, including a website, email, virtual private network, or custom application.

''(9) RANSOMWARE INCIDENT.—The term 'ransomware incident' means an incident that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system for the purpose of coercing the information system's owner, operator, or another person.

''(9) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term 'State and Local Cybersecurity Grant Program' means the program established under subsection (b).

''(10) STATE AND LOCAL CYBERSECURITY RESILIENCE COMMITTEE.—The term 'State and Local

Cybersecurity Resilience Committee' means the committee established under subsection (o)(1).

''(b) ESTABLISHMENT.—

''(1) IN GENERAL.—The Secretary, acting through the Director, shall establish a program, to be known as the 'the State and Local Cybersecurity Grant Program', to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations.

''(2) APPLICATION.—An eligible entity seeking a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

''(c) BASELINE REQUIREMENTS.—An eligible entity or multistate group that receives a grant under this section shall use the grant in compliance with—

''(1)(A) the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group; and

''(B) the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and

Territorial Governments developed under section 2210(e)(1); or

''(2) activities carried out under paragraphs (3), (4), and (5) of subsection (h).

''(d) ADMINISTRATION.—The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 2003 and 2004.

''(e) CYBERSECURITY PLANS.—

''(1) IN GENERAL.—An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for approval.

''(2) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

''(A) incorporate, to the extent practicable, any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations;

''(B) describe, to the extent practicable, how the eligible entity will—

''(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal

organizations within the jurisdiction of the eligible entity and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

''(ii) monitor, audit, and track activity between information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and between those information systems and information systems not owned or operated by the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity;

''(iii) enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or local or Tribal organizations against cybersecurity risks and cybersecurity threats;

''(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems of the eligible entity or local or Tribal organizations;

''(v) ensure that State, local, and Tribal organizations that own or operate information systems that are located within the jurisdiction of the eligible entity—

''(I) adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by, and the cyber supply chain risk management best practices identified by, the National Institute of Standards and Technology; and

''(II) utilize knowledge bases of adversary tools and tactics to assess risk;

''(vi) promote the delivery of safe, recognizable, and trustworthy online services by State, local, and Tribal organizations,

including through the use of the .gov internet domain;

''(vii) ensure continuity of operations of the eligible entity and local, and Tribal organizations in the event of a cybersecurity incident (including a ransomware incident), including by conducting exercises to practice responding to such an incident;

''(viii) use the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of State, local, or Tribal organizations, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, and Tribal organization personnel to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

''(ix) ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the el-

igible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity in the event of an incident involving such communications or data networks within the jurisdiction of the eligible entity;

''(x) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats related to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity;

''(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity, including by expanding existing information sharing agreements with the Department;

''(xii) enhance the capability of the eligible entity to share cyber threat indictors and related information with the Department;

"(xiii) leverage cybersecurity services offered by the Department;

"(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats to information systems of the eligible entity in consultation with—

"(I) local and Tribal organizations within the jurisdiction of the eligible entity; and

"(II) as applicable—

"(aa) States that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an information sharing and analysis organization; and

"(bb) countries that neighbor the jurisdiction of the eligible entity; and

"(xv) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

''(C) describe, to the extent practicable, the individual responsibilities of the eligible entity and local and Tribal organizations within the jurisdiction of the eligible entity in implementing the plan;

''(D) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

''(E) describe how the eligible entity will measure progress towards implementing the plan.

''(3) DISCRETIONARY ELEMENTS.—A Cybersecurity Plan of an eligible entity may include a description of—

''(A) cooperative programs developed by groups of local and Tribal organizations within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

''(B) programs provided by the eligible entity to support local and Tribal organizations and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

''(4) MANAGEMENT OF FUNDS.—An eligible entity applying for a grant under this section shall agree to designate the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity as the primary official for the management and allocation of funds awarded under this section.

''(f) MULTISTATE GRANTS.—

''(1) IN GENERAL.—The Secretary, acting through the Director, may award grants under this section to a group of two or more eligible entities to support multistate efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities.

''(2) SATISFACTION OF OTHER REQUIREMENTS.—In order to be eligible for a multistate grant under this subsection, each eligible entity that comprises a multistate group shall submit to the Secretary—

''(A) a Cybersecurity Plan for approval in accordance with subsection (i); and

''(B) a plan for establishing a cybersecurity planning committee under subsection (g).

''(3) APPLICATION.—

"(A) IN GENERAL.—A multistate group applying for a multistate grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

"(B) MULTISTATE PROJECT DESCRIPTION.—An application of a multistate group under subparagraph (A) shall include a plan describing—

"(i) the division of responsibilities among the eligible entities that comprise the multistate group for administering the grant for which application is being made;

"(ii) the distribution of funding from such a grant among the eligible entities that comprise the multistate group; and

"(iii) how the eligible entities that comprise the multistate group will work together to implement the Cybersecurity Plan of each of those eligible entities.

"(g) PLANNING COMMITTEES.—

"(1) IN GENERAL.—An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

"(A) assist in the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

"(B) approve the Cybersecurity Plan of the eligible entity; and

"(C) assist in the determination of effective funding priorities for a grant under this section in accordance with subsection (h).

"(2) COMPOSITION.—A committee of an eligible entity established under paragraph (1) shall—

"(A) be comprised of representatives from the eligible entity and counties, cities, towns, Tribes, and public educational and health institutions within the jurisdiction of the eligible entity; and

"(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

"(3) CYBERSECURITY EXPERTISE.—Not less than ½ of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

"(4) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this

subsection may be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that meets, or may be leveraged to meet, the requirements of this subsection.

''(h) USE OF FUNDS.—An eligible entity that receives a grant under this section shall use the grant to—

''(1) implement the Cybersecurity Plan of the eligible entity;

''(2) develop or revise the Cybersecurity Plan of the eligible entity; or

''(3) assist with activities that address imminent cybersecurity risks or cybersecurity threats to the information systems of the eligible entity or a local or Tribal organization within the jurisdiction of the eligible entity.

''(i) APPROVAL OF PLANS.—

''(1) APPROVAL AS CONDITION OF GRANT.—Before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall review the Cybersecurity Plan, or any revisions thereto, of the eligible entity and approve such plan, or revised plan, if it satisfies the requirements specified in paragraph (2).

''(2) PLAN REQUIREMENTS.—In approving a Cybersecurity Plan of an eligible entity under this subsection, the Director shall ensure that the Cybersecurity Plan—

''(A) satisfies the requirements of subsection (e)(2);

''(B) upon the issuance of the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments authorized pursuant to section 2210(e), complies, as appropriate, with the goals and objectives of the strategy; and

''(C) has been approved by the cybersecurity planning committee of the eligible entity established under subsection (g).

''(3) APPROVAL OF REVISIONS.—The Secretary, acting through the Director, may approve revisions to a Cybersecurity Plan as the Director determines appropriate.

''(4) EXCEPTION.—Notwithstanding subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary if—

''(A) the eligible entity certifies to the Secretary that—

''(i) the activities that will be supported by the grant are integral to the development of the Cybersecurity Plan of the eligible entity; and

''(ii) the eligible entity will submit by September 30, 2023, to the Secretary a Cybersecurity Plan for review, and if appropriate, approval; or

''(B) the eligible entity certifies to the Secretary, and the Director confirms, that the eligible entity will use funds from the grant to assist with the activities described in subsection (h)(3).

''(j) LIMITATIONS ON USES OF FUNDS.—

''(1) IN GENERAL.—An eligible entity that receives a grant under this section may not use the grant—

''(A) to supplant State, local, or Tribal funds;

''(B) for any recipient cost-sharing contribution;

''(C) to pay a demand for ransom in an attempt to—

''(i) regain access to information or an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity; or

''(ii) prevent the disclosure of information that has been removed without authorization from an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity;

''(D) for recreational or social purposes; or

''(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity.

''(2) PENALTIES.—In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant under this section uses the grant for the purposes for which the grant is awarded.

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1) may be construed to prohibit the use of grant funds provided to a State, local, or Tribal organization for otherwise permissible uses under

this section on the basis that a State, local, or Tribal organization has previously used State, local, or Tribal funds to support the same or similar uses.

''(k) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct defects, if any, in such applications before making final awards.

''(l) APPORTIONMENT.—For fiscal year 2022 and each fiscal year thereafter, the Secretary shall apportion amounts appropriated to carry out this section among States as follows:

''(1) BASELINE AMOUNT.—The Secretary shall first apportion 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the U.S. Virgin Islands, and 0.75 percent of such amounts to each of the remaining States.

''(2) REMAINDER.—The Secretary shall apportion the remainder of such amounts in the ratio that—

''(A) the population of each eligible entity, bears to

''(B) the population of all eligible entities.

"(3) MINIMUM ALLOCATION TO INDIAN TRIBES.—

"(A) IN GENERAL.—In apportioning amounts under this section, the Secretary shall ensure that, for each fiscal year, directly eligible Tribes collectively receive, from amounts appropriated under the State and Local Cybersecurity Grant Program, not less than an amount equal to three percent of the total amount appropriated for grants under this section.

"(B) ALLOCATION.—Of the amount reserved under subparagraph (A), funds shall be allocated in a manner determined by the Secretary in consultation with Indian tribes.

"(C) EXCEPTION.—This paragraph shall not apply in any fiscal year in which the Secretary—

"(i) receives fewer than five applications from Indian tribes; or

"(ii) does not approve at least two application from Indian tribes.

"(m) FEDERAL SHARE.—

"(1) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made

available with a grant under this section may not exceed—

''(A) in the case of a grant to an eligible entity—

''(i) for fiscal year 2022, 90 percent;

''(ii) for fiscal year 2023, 80 percent;

''(iii) for fiscal year 2024, 70 percent;

''(iv) for fiscal year 2025, 60 percent; and

''(v) for fiscal year 2026 and each subsequent fiscal year, 50 percent; and

''(B) in the case of a grant to a multistate group—

''(i) for fiscal year 2022, 95 percent;

''(ii) for fiscal year 2023, 85 percent;

''(iii) for fiscal year 2024, 75 percent;

''(iv) for fiscal year 2025, 65 percent; and

''(v) for fiscal year 2026 and each subsequent fiscal year, 55 percent.

''(2) WAIVER.—The Secretary may waive or modify the requirements of paragraph (1) for an Indian tribe if the Secretary determines such a waiver is in the public interest.

''(n) RESPONSIBILITIES OF GRANTEES.—

''(1) CERTIFICATION.—Each eligible entity or multistate group that receives a grant under this section shall certify to the Secretary that the grant will be used—

''(A) for the purpose for which the grant is awarded; and

''(B) in compliance with, as the case may be—

''(i) the Cybersecurity Plan of the eligible entity;

''(ii) the Cybersecurity Plans of the eligible entities that comprise the multistate group; or

''(iii) a purpose approved by the Secretary under subsection (h) or pursuant to an exception under subsection (i).

''(2) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—Not later than 45 days after the date on which an eligible entity or multistate group receives a grant under this section, the eligible entity or multistate group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local and Tribal organizations within the jurisdiction of the eligible entity or

the eligible entities that comprise the multistate group, and as applicable, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group—

''(A) not less than 80 percent of funds available under the grant;

''(B) with the consent of the local and Tribal organizations, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

''(C) with the consent of the local and Tribal organizations, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

''(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—An eligible entity or multistate group shall certify to the Secretary that the eligible entity or multistate group has made the distribution to local, Tribal, and territorial governments required under paragraph (2).

''(4) EXTENSION OF PERIOD.—

''(A) IN GENERAL.—An eligible entity or multistate group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

''(B) APPROVAL.—The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity Grant Program.

''(5) EXCEPTION.—Paragraph (2) shall not apply to the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the Virgin Islands, or an Indian tribe.

''(6) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local or Tribal organization required in accordance with paragraph (2), the local or Tribal organization may petition the Secretary to request that grant funds be provided directly to the local or Tribal organization.

''(7) PENALTIES.—In addition to other remedies available to the Secretary, the Secretary may

terminate or reduce the amount of a grant awarded under this section to an eligible entity or distribute grant funds previously awarded to such eligible entity directly to the appropriate local or Tribal organization as a replacement grant in an amount the Secretary determines appropriate if such eligible entity violates a requirement of this subsection.

''(o) ADVISORY COMMITTEE.—

''(1) ESTABLISHMENT.—Not later than 120 days after the date of enactment of this section, the Director shall establish a State and Local Cybersecurity Resilience Committee to provide State, local, and Tribal stakeholder expertise, situational awareness, and recommendations to the Director, as appropriate, regarding how to—

''(A) address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations; and

''(B) improve the ability of State, local, and Tribal organizations to prevent, protect against, respond to, mitigate, and recover from such cybersecurity risks and cybersecurity threats.

''(2) DUTIES.—The committee established under paragraph (1) shall—

"(A) submit to the Director recommendations that may inform guidance for applicants for grants under this section;

"(B) upon the request of the Director, provide to the Director technical assistance to inform the review of Cybersecurity Plans submitted by applicants for grants under this section, and, as appropriate, submit to the Director recommendations to improve those plans prior to the approval of the plans under subsection (i);

"(C) advise and provide to the Director input regarding the Homeland Security Strategy to Improve Cybersecurity for State, Local, Tribal, and Territorial Governments required under section 2210;

"(D) upon the request of the Director, provide to the Director recommendations, as appropriate, regarding how to—

"(i) address cybersecurity risks and cybersecurity threats on information systems of State, local, or Tribal organizations; and

"(ii) improve the cybersecurity resilience of State, local, or Tribal organizations; and

"(E) regularly coordinate with the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

"(3) MEMBERSHIP.—

"(A) NUMBER AND APPOINTMENT.—The State and Local Cybersecurity Resilience Committee established pursuant to paragraph (1) shall be composed of 15 members appointed by the Director, as follows:

"(i) Two individuals recommended to the Director by the National Governors Association.

"(ii) Two individuals recommended to the Director by the National Association of State Chief Information Officers.

"(iii) One individual recommended to the Director by the National Guard Bureau.

''(iv) Two individuals recommended to the Director by the National Association of Counties.

''(v) One individual recommended to the Director by the National League of Cities.

''(vi) One individual recommended to the Director by the United States Conference of Mayors.

''(vii) One individual recommended to the Director by the Multi-State Information Sharing and Analysis Center.

''(viii) One individual recommended to the Director by the National Congress of American Indians.

''(viii) Four individuals who have educational and professional experience relating to cybersecurity work or cybersecurity policy.

''(B) TERMS.—

''(i) IN GENERAL.—Subject to clause (ii), each member of the State and Local Cybersecurity Resilience Committee shall be appointed for a term of two years.

''(ii) REQUIREMENT.—At least two members of the State and Local Cybersecurity Resilience Committee shall also be members of the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

''(iii) EXCEPTION.—A term of a member of the State and Local Cybersecurity Resilience Committee shall be three years if the member is appointed initially to the Committee upon the establishment of the Committee.

''(iv) TERM REMAINDERS.—Any member of the State and Local Cybersecurity Resilience Committee appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of such term. A member may serve after the expiration of such member's term until a successor has taken office.

"(v) VACANCIES.—A vacancy in the State and Local Cybersecurity Resilience Committee shall be filled in the manner in which the original appointment was made.

"(C) PAY.—Members of the State and Local Cybersecurity Resilience Committee shall serve without pay.

"(4) CHAIRPERSON; VICE CHAIRPERSON.—The members of the State and Local Cybersecurity Resilience Committee shall select a chairperson and vice chairperson from among members of the committee.

"(5) PERMANENT AUTHORITY.—Notwithstanding section 14 of the Federal Advisory Committee Act (5 U.S.C. App.), the State and Local Cybersecurity Resilience Committee shall be a permanent authority.

"(p) REPORTS.—

"(1) ANNUAL REPORTS BY GRANT RECIPIENTS.—

"(A) IN GENERAL.—Not later than one year after an eligible entity or multistate group receives funds under this section, the eligible entity or multistate group shall submit to the Secretary a report on the progress of the eligible entity or multistate group in implementing

the Cybersecurity Plan of the eligible entity or Cybersecurity Plans of the eligible entities that comprise the multistate group, as the case may be.

''(B) ABSENCE OF PLAN.—Not later than 180 days after an eligible entity that does not have a Cybersecurity Plan receives funds under this section for developing its Cybersecurity Plan, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds during the fiscal year to—

''(i) so develop such a Cybersecurity Plan; or

''(ii) assist with the activities described in subsection (h)(3).

''(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than once per year, the Secretary, acting through the Director, shall submit to Congress a report on the use of grants awarded under this section and any progress made toward the following:

''(A) Achieving the objectives set forth in the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Ter-

ritorial Governments, upon the date on which the strategy is issued under section 2210.

''(B) Developing, implementing, or revising Cybersecurity Plans.

''(C) Reducing cybersecurity risks and cybersecurity threats to information systems, applications, and user accounts owned or operated by or on behalf of State, local, and Tribal organizations as a result of the award of such grants.

''(q) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

''(1) for each of fiscal years 2022 through 2026, $500,000,000; and

''(2) for each subsequent fiscal year, such sums as may be necessary.

''SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

''The Secretary, acting through the Director, shall develop, regularly update, and maintain a resource guide for use by State, local, Tribal, and territorial government officials, including law enforcement officers, to help such officials identify, prepare for, detect, protect against, re-

spond to, and recover from cybersecurity risks (as such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209).''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 4, is further amended by inserting after the item relating to section 2220 the following new items:

''Sec. 2220A. State and Local Cybersecurity Grant Program.
''Sec. 2220B. Cybersecurity resource guide development for State, local, Tribal, and territorial government officials.''.

SEC. 3. STRATEGY.

(a) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.—Section 2210 of the Homeland Security Act of 2002 (6 U.S.C. 660) is amended by adding at the end the following new subsection:

''(e) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.—

''(1) IN GENERAL.—

''(A) REQUIREMENT.—Not later than one year after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State

and Local Cybersecurity Resilience Committee established under section 2220A, and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

''(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall—

''(i) provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks (as such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209); and

''(ii) establish baseline requirements for cybersecurity plans under this section and principles with which such plans shall align.

''(2) CONTENTS.—The strategy required under paragraph (1) shall—

''(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

''(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State

Information Sharing and Analysis Center, to improve—

''(i) incident exercises, information sharing and incident notification procedures;

''(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

''(iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40, United States Code;

''(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover

from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents; and

''(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

''(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, and other stakeholders, as appropriate, shall consider—

''(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

''(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

''(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems (as such term is defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)) owned or operated by State, local, Tribal, and territorial governments;

''(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies; and

''(E) recommendations made by the State and Local Cybersecurity Resilience Committee established under section 2220A.

''(4) EXEMPTION.—Chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), shall not apply to any action to implement this subsection.''.

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

(1) by redesignating subsections (d) through (i) as subsections (e) through (j), respectively; and

(2) by inserting after subsection (c) the following new subsection:

''(d) ADDITIONAL RESPONSIBILITIES.—In addition to the responsibilities under subsection (c), the Director shall—

''(1) develop program guidance, in consultation with the State and Local Government Cybersecurity Resilience Committee established under section 2220A, for the State and Local Cybersecurity Grant Program under such section or any other homeland security assistance administered by the Department to improve cybersecurity;

''(2) review, in consultation with the State and Local Cybersecurity Resilience Committee, all cybersecurity plans of State, local, Tribal, and territorial governments developed pursuant to any homeland security assistance administered by the Department to improve cybersecurity;

''(3) provide expertise and technical assistance to State, local, Tribal, and territorial government officials with respect to cybersecurity; and

''(4) provide education, training, and capacity development to enhance the security and resilience of cybersecurity and infrastructure security.''.

(c) FEASIBILITY STUDY.—Not later than 270 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security of the Department of Homeland Security shall conduct a study to assess the feasibility of implementing a short-term rotational program for the detail to the Agency of approved State, local, Tribal, and territorial government employees in cyber workforce positions.

SEC. 4. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

(1) HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

"SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.";

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

"SEC. 2216. JOINT CYBER PLANNING OFFICE.";

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";

(D) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".

(2) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter pre-

ceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint cyber planning office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.''.

Amendments to H.R. 3243

AMENDMENT TO H.R. 3243

OFFERED BY MRS. WATSON COLEMAN OF NEW JERSEY

Strike ''pipeline security section'' and insert ''pipeline security division'' each place such term appears.

Page 3, line 7, strike ''section'' and insert ''division''.

Page 3, line 21, strike ''section'' and insert ''division''.

Page 3, line 21, insert ''in the executive service of the Administration'' after ''individual''.

Page 3, line 24, strike ''section''and insert ''division''.

Page 4, line 1, strike ''section'' and insert ''division''.

Page 4, line 2, strike ''section'' and insert ''division''.

Page 5, line 22, strike ''section's'' and insert ''division's''.

☒

AMENDMENT TO H.R. 3243

OFFERED BY MR. THOMPSON OF MISSISSIPPI

Page 4, line 22, insert before the period the following: ", unless such guidelines are superseded by directives or regulations".

Page 5, beginning line 5, strike "to provide recommendations" and insert ", or mandatory security assessments if required by superseding directives or regulations, to provide recommendations or requirements".

Page 5, line 18, insert before the period the following: "or superseding directives or regulations".

Page 5, strike lines 19 through 21 and insert the following:

"(6) Supporting the development and implementation of a security directive or regulation when the Administrator issues such a directive or regulation.".

Page 6, line 11, insert before the period the following: ", except to the extent such guidelines have been superseded by directives or regulations".

Page 8, line 18, insert ''directives, regulations,'' after ''guidelines,''.

☒

AMENDMENT TO H.R. 3243

OFFERED BY MS. SLOTKIN OF MICHIGAN

Page 7, beginning line 25, insert the following:

(c) CYBERSECURITY EXPERTISE.—The strategy shall include an assessment of the cybersecurity expertise determined necessary by the Administrator of the Transportation Security Administration and a plan for developing such expertise within the Administration.