

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:

1                   “(F) The Office for Civil Rights and Civil  
2                   Liberties.

3                   “(G) The Privacy Office.”.

Page 3, after line 10, insert the following:

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

7                   “(A) The Board’s mission, goals, and  
8                   scope of its activities.

9                   “(B) The duties of the Board’s representa-  
10                  tives.

11                  “(C) The frequency of the Board’s meet-  
12                  ings.”.

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:

**1 SECTION 1. SHORT TITLE.**

2       This Act may be cited as the “Cybersecurity Vulner-  
3 ability Remediation Act”.

**4 SEC. 2. CYBERSECURITY VULNERABILITIES.**

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

7           (1) in subsection (a)—

8               (A) in paragraph (5), by striking “and”  
9               after the semicolon at the end;

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

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

14               “(6) the term ‘cybersecurity vulnerability’ has  
15               the meaning given the term ‘security vulnerability’  
16               in section 102 of the Cybersecurity Information  
17               Sharing Act of 2015 (6 U.S.C. 1501); and”.

18            (2) in subsection (c)—

- 1 (A) in paragraph (5)—
- 2 (i) in subparagraph (A), by striking
- 3 “and” after the semicolon at the end;
- 4 (ii) by redesignating subparagraph
- 5 (B) as subparagraph (C);
- 6 (iii) by inserting after subparagraph
- 7 (A) the following new subparagraph:
- 8 “(B) sharing mitigation protocols to counter cy-
- 9 bersecurity vulnerabilities pursuant to subsection
- 10 (n); and”; and
- 11 (iv) in subparagraph (C), as so reded-
- 12 igned, by inserting “and mitigation pro-
- 13 tocols to counter cybersecurity
- 14 vulnerabilities in accordance with subpara-
- 15 graph (B)” before “with Federal”;
- 16 (B) in paragraph (7)(C), by striking
- 17 “sharing” and inserting “share”; and
- 18 (C) in paragraph (9), by inserting “mitiga-
- 19 tion protocols to counter cybersecurity
- 20 vulnerabilities,” after “measures,”;
- 21 (3) in subsection (e)(1)(G), by striking the
- 22 semicolon after “and” at the end;
- 23 (4) by redesignating subsection (o) as sub-
- 24 section (p); and

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

3           “(o) **PROTOCOLS TO COUNTER CERTAIN CYBERSE-**  
4 **CURITY VULNERABILITIES.**—The Director may, as appro-  
5 priate, identify, develop, and disseminate actionable proto-  
6 cols to mitigate cybersecurity vulnerabilities to informa-  
7 tion systems and industrial control systems, including in  
8 circumstances in which such vulnerabilities exist because  
9 software or hardware is no longer supported by a ven-  
10 dor.”.

11 **SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.**

12           (a) **REPORT.**—Not later than one year after the date  
13 of the enactment of this Act, the Director of the Cyberse-  
14 curity and Infrastructure Security Agency of the Depart-  
15 ment of Homeland Security shall submit to the Committee  
16 on Homeland Security of the House of Representatives  
17 and the Committee on Homeland Security and Govern-  
18 mental Affairs of the Senate a report on how the Agency  
19 carries out subsection (n) of section 2209 of the Homeland  
20 Security Act of 2002 to coordinate vulnerability disclo-  
21 sures, including disclosures of cybersecurity vulnerabilities  
22 (as such term is defined in such section), and subsection  
23 (o) of such section (as added by section 2) to disseminate  
24 actionable protocols to mitigate cybersecurity

1 vulnerabilities to information systems and industrial con-  
2 trol systems, that includes the following:

3 (1) A description of the policies and procedures  
4 relating to the coordination of vulnerability disclo-  
5 sures.

6 (2) A description of the levels of activity in fur-  
7 therance of such subsections (n) and (o) of such sec-  
8 tion 2209.

9 (3) Any plans to make further improvements to  
10 how information provided pursuant to such sub-  
11 sections can be shared (as such term is defined in  
12 such section 2209) between the Department and in-  
13 dustry and other stakeholders.

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

17 (5) A description of how privacy and civil lib-  
18 erties are preserved in the collection, retention, use,  
19 and sharing of vulnerability disclosures.

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

1 **SEC. 4. COMPETITION RELATING TO CYBERSECURITY**  
2 **VULNERABILITIES.**

3 The Under Secretary for Science and Technology of  
4 the Department of Homeland Security, in consultation  
5 with the Director of the Cybersecurity and Infrastructure  
6 Security Agency of the Department, may establish an in-  
7 centive-based program that allows industry, individuals,  
8 academia, and others to compete in identifying remedi-  
9 ation solutions for cybersecurity vulnerabilities (as such  
10 term is defined in section 2209 of the Homeland Security  
11 Act of 2002, as amended by section 2) to information sys-  
12 tems (as such term is defined in such section 2209) and  
13 industrial control systems, including supervisory control  
14 and data acquisition systems.

15 **SEC. 5. TITLE XXII TECHNICAL AND CLERICAL AMEND-**  
16 **MENTS.**

17 (a) TECHNICAL AMENDMENTS.—

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

21 (A) in the first section 2215 (6 U.S.C.  
22 665; relating to the duties and authorities relat-  
23 ing to .gov internet domain), by amending the  
24 section enumerator and heading to read as fol-  
25 lows:



1 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**  
2 **INTERNET DOMAIN.”;**

3 (B) in the second section 2215 (6 U.S.C.  
4 665b; relating to the joint cyber planning of-  
5 fice), by amending the section enumerator and  
6 heading to read as follows:

7 **“SEC. 2216. JOINT CYBER PLANNING OFFICE.”;**

8 (C) in the third section 2215 (6 U.S.C.  
9 665c; relating to the Cybersecurity State Coor-  
10 dinator), by amending the section enumerator  
11 and heading to read as follows:

12 **“SEC. 2217. CYBERSECURITY STATE COORDINATOR.”;**

13 (D) in the fourth section 2215 (6 U.S.C.  
14 665d; relating to Sector Risk Management  
15 Agencies), by amending the section enumerator  
16 and heading to read as follows:

17 **“SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.”;**

18 (E) in section 2216 (6 U.S.C. 665e; relat-  
19 ing to the Cybersecurity Advisory Committee),  
20 by amending the section enumerator and head-  
21 ing to read as follows:

22 **“SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.”; and**

23 (F) in section 2217 (6 U.S.C. 665f; relat-  
24 ing to Cybersecurity Education and Training  
25 Programs), by amending the section enu-  
26 merator and heading to read as follows:

1 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**  
2 **PROGRAMS.”.**

3 (2) CONSOLIDATED APPROPRIATIONS ACT,  
4 2021.—Paragraph (1) of section 904(b) of division U  
5 of the Consolidated Appropriations Act, 2021 (Pub-  
6 lic Law 116–260) is amended, in the matter pre-  
7 ceding subparagraph (A), by inserting “of 2002”  
8 after “Homeland Security Act”.

9 (b) CLERICAL AMENDMENT.—The table of contents  
10 in section 1(b) of the Homeland Security Act of 2002 is  
11 amended by striking the items relating to sections 2214  
12 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:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “State and Local Cyber-  
3 security Improvement Act”.

**4 SEC. 2. STATE AND LOCAL CYBERSECURITY GRANT PRO-  
5 GRAM.**

6 (a) IN GENERAL.—Subtitle A of title XXII of the  
7 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)  
8 is amended by adding at the end the following new sec-  
9 tions:

**10 “SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT  
11 PROGRAM.**

12 “(a) DEFINITIONS.—In this section:

13 “(1) CYBER THREAT INDICATOR.—The term  
14 ‘cyber threat indicator’ has the meaning given the  
15 term in section 102 of the Cybersecurity Act of 2015  
16 (6 U.S.C. 1501).

1           “(2) CYBERSECURITY PLAN.—The term ‘Cyber-  
2           security Plan’ means a plan submitted by an eligible  
3           entity under subsection (e)(1).

4           “(3) ELIGIBLE ENTITY.—The term ‘eligible en-  
5           tity’ means—

6                   “(A) a State; or

7                   “(B) an Indian tribe that, not later than  
8                   120 days after the date of the enactment of this  
9                   section or not later than 120 days before the  
10                  start of any fiscal year in which a grant under  
11                  this section is awarded—

12                           “(i) notifies the Secretary that the In-  
13                           dian tribe intends to develop a Cybersecu-  
14                           rity Plan; and

15                           “(ii) agrees to forfeit any distribution  
16                           under subsection (n)(2).

17           “(4) INCIDENT.—The term ‘incident’ has the  
18           meaning given the term in section 2209.

19           “(5) INDIAN TRIBE; TRIBAL ORGANIZATION.—  
20           The term ‘Indian tribe’ or ‘Tribal organization’ has  
21           the meaning given that term in section 4(e) of the  
22           of the Indian Self-Determination and Education As-  
23           sistance Act (25 U.S.C. 5304(e)).

24           “(6) INFORMATION SHARING AND ANALYSIS OR-  
25           GANIZATION.—The term ‘information sharing and

1 analysis organization’ has the meaning given the  
2 term in section 2222.

3 “(7) INFORMATION SYSTEM.—The term ‘infor-  
4 mation system’ has the meaning given the term in  
5 section 102 of the Cybersecurity Act of 2015 (6  
6 U.S.C. 1501).

7 “(8) ONLINE SERVICE.—The term ‘online serv-  
8 ice’ means any internet-facing service, including a  
9 website, email, virtual private network, or custom  
10 application.

11 “(9) RANSOMWARE INCIDENT.—The term  
12 ‘ransomware incident’ means an incident that actu-  
13 ally or imminently jeopardizes, without lawful au-  
14 thority, the integrity, confidentiality, or availability  
15 of information on an information system, or actually  
16 or imminently jeopardizes, without lawful authority,  
17 an information system for the purpose of coercing  
18 the information system’s owner, operator, or another  
19 person.

20 “(9) STATE AND LOCAL CYBERSECURITY GRANT  
21 PROGRAM.—The term ‘State and Local Cybersecu-  
22 rity Grant Program’ means the program established  
23 under subsection (b).

24 “(10) STATE AND LOCAL CYBERSECURITY RE-  
25 SILIENCE COMMITTEE.—The term ‘State and Local

1 Cybersecurity Resilience Committee’ means the com-  
2 mittee established under subsection (o)(1).

3 “(b) ESTABLISHMENT.—

4 “(1) IN GENERAL.—The Secretary, acting  
5 through the Director, shall establish a program, to  
6 be known as the ‘the State and Local Cybersecurity  
7 Grant Program’, to award grants to eligible entities  
8 to address cybersecurity risks and cybersecurity  
9 threats to information systems of State, local, or  
10 Tribal organizations.

11 “(2) APPLICATION.—An eligible entity seeking  
12 a grant under the State and Local Cybersecurity  
13 Grant Program shall submit to the Secretary an ap-  
14 plication at such time, in such manner, and con-  
15 taining such information as the Secretary may re-  
16 quire.

17 “(c) BASELINE REQUIREMENTS.—An eligible entity  
18 or multistate group that receives a grant under this sec-  
19 tion shall use the grant in compliance with—

20 “(1)(A) the Cybersecurity Plan of the eligible  
21 entity or the Cybersecurity Plans of the eligible enti-  
22 ties that comprise the multistate group; and

23 “(B) the Homeland Security Strategy to Im-  
24 prove the Cybersecurity of State, Local, Tribal, and

1 Territorial Governments developed under section  
2 2210(e)(1); or

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

5 “(d) ADMINISTRATION.—The State and Local Cyber-  
6 security Grant Program shall be administered in the same  
7 office of the Department that administers grants made  
8 under sections 2003 and 2004.

9 “(e) CYBERSECURITY PLANS.—

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

13 “(2) REQUIRED ELEMENTS.—A Cybersecurity  
14 Plan of an eligible entity shall—

15 “(A) incorporate, to the extent practicable,  
16 any existing plans of the eligible entity to pro-  
17 tect against cybersecurity risks and cybersecu-  
18 rity threats to information systems of State,  
19 local, or Tribal organizations;

20 “(B) describe, to the extent practicable,  
21 how the eligible entity will—

22 “(i) manage, monitor, and track infor-  
23 mation systems, applications, and user ac-  
24 counts owned or operated by or on behalf  
25 of the eligible entity or by local or Tribal



1 organizations within the jurisdiction of the  
2 eligible entity and the information tech-  
3 nology deployed on those information sys-  
4 tems, including legacy information systems  
5 and information technology that are no  
6 longer supported by the manufacturer of  
7 the systems or technology;

8 “(ii) monitor, audit, and track activity  
9 between information systems, applications,  
10 and user accounts owned or operated by or  
11 on behalf of the eligible entity or by local  
12 or Tribal organizations within the jurisdic-  
13 tion of the eligible entity and between  
14 those information systems and information  
15 systems not owned or operated by the eligi-  
16 ble entity or by local or Tribal organiza-  
17 tions within the jurisdiction of the eligible  
18 entity;

19 “(iii) enhance the preparation, re-  
20 sponse, and resilience of information sys-  
21 tems, applications, and user accounts  
22 owned or operated by or on behalf of the  
23 eligible entity or local or Tribal organiza-  
24 tions against cybersecurity risks and cyber-  
25 security threats;

1           “(iv) implement a process of contin-  
2           uous cybersecurity vulnerability assess-  
3           ments and threat mitigation practices  
4           prioritized by degree of risk to address cy-  
5           bersecurity risks and cybersecurity threats  
6           on information systems of the eligible enti-  
7           ty or local or Tribal organizations;

8           “(v) ensure that State, local, and  
9           Tribal organizations that own or operate  
10          information systems that are located with-  
11          in the jurisdiction of the eligible entity—

12                 “(I) adopt best practices and  
13                 methodologies to enhance cybersecu-  
14                 rity, such as the practices set forth in  
15                 the cybersecurity framework developed  
16                 by, and the cyber supply chain risk  
17                 management best practices identified  
18                 by, the National Institute of Stand-  
19                 ards and Technology; and

20                 “(II) utilize knowledge bases of  
21                 adversary tools and tactics to assess  
22                 risk;

23           “(vi) promote the delivery of safe, rec-  
24           ognizable, and trustworthy online services  
25           by State, local, and Tribal organizations,

1 including through the use of the .gov inter-  
2 net domain;

3 “(vii) ensure continuity of operations  
4 of the eligible entity and local, and Tribal  
5 organizations in the event of a cybersecu-  
6 rity incident (including a ransomware inci-  
7 dent), including by conducting exercises to  
8 practice responding to such an incident;

9 “(viii) use the National Initiative for  
10 Cybersecurity Education Cybersecurity  
11 Workforce Framework developed by the  
12 National Institute of Standards and Tech-  
13 nology to identify and mitigate any gaps in  
14 the cybersecurity workforces of State,  
15 local, or Tribal organizations, enhance re-  
16 cruitment and retention efforts for such  
17 workforces, and bolster the knowledge,  
18 skills, and abilities of State, local, and  
19 Tribal organization personnel to address  
20 cybersecurity risks and cybersecurity  
21 threats, such as through cybersecurity hy-  
22 giene training;

23 “(ix) ensure continuity of communica-  
24 tions and data networks within the juris-  
25 diction of the eligible entity between the el-

1 eligible entity and local and Tribal organiza-  
2 tions that own or operate information sys-  
3 tems within the jurisdiction of the eligible  
4 entity in the event of an incident involving  
5 such communications or data networks  
6 within the jurisdiction of the eligible entity;

7 “(x) assess and mitigate, to the great-  
8 est degree possible, cybersecurity risks and  
9 cybersecurity threats related to critical in-  
10 frastructure and key resources, the deg-  
11 radation of which may impact the perform-  
12 ance of information systems within the ju-  
13 risdiction of the eligible entity;

14 “(xi) enhance capabilities to share  
15 cyber threat indicators and related infor-  
16 mation between the eligible entity and local  
17 and Tribal organizations that own or oper-  
18 ate information systems within the juris-  
19 diction of the eligible entity, including by  
20 expanding existing information sharing  
21 agreements with the Department;

22 “(xii) enhance the capability of the el-  
23 igible entity to share cyber threat indictors  
24 and related information with the Depart-  
25 ment;

1           “(xiii) leverage cybersecurity services  
2           offered by the Department;

3           “(xiv) develop and coordinate strate-  
4           gies to address cybersecurity risks and cy-  
5           bersecurity threats to information systems  
6           of the eligible entity in consultation with—

7                   “(I) local and Tribal organiza-  
8                   tions within the jurisdiction of the eli-  
9                   gible entity; and

10                   “(II) as applicable—

11                           “(aa) States that neighbor  
12                           the jurisdiction of the eligible en-  
13                           tity or, as appropriate, members  
14                           of an information sharing and  
15                           analysis organization; and

16                           “(bb) countries that neigh-  
17                           bor the jurisdiction of the eligible  
18                           entity; and

19           “(xv) implement an information tech-  
20           nology and operational technology mod-  
21           ernization cybersecurity review process  
22           that ensures alignment between informa-  
23           tion technology and operational technology  
24           cybersecurity objectives;

1           “(C) describe, to the extent practicable, the  
2 individual responsibilities of the eligible entity  
3 and local and Tribal organizations within the  
4 jurisdiction of the eligible entity in imple-  
5 menting the plan;

6           “(D) outline, to the extent practicable, the  
7 necessary resources and a timeline for imple-  
8 menting the plan; and

9           “(E) describe how the eligible entity will  
10 measure progress towards implementing the  
11 plan.

12           “(3) DISCRETIONARY ELEMENTS.—A Cyberse-  
13 curity Plan of an eligible entity may include a de-  
14 scription of—

15           “(A) cooperative programs developed by  
16 groups of local and Tribal organizations within  
17 the jurisdiction of the eligible entity to address  
18 cybersecurity risks and cybersecurity threats;  
19 and

20           “(B) programs provided by the eligible en-  
21 tity to support local and Tribal organizations  
22 and owners and operators of critical infrastruc-  
23 ture to address cybersecurity risks and cyberse-  
24 curity threats.

1           “(4) MANAGEMENT OF FUNDS.—An eligible en-  
2           tity applying for a grant under this section shall  
3           agree to designate the Chief Information Officer, the  
4           Chief Information Security Officer, or an equivalent  
5           official of the eligible entity as the primary official  
6           for the management and allocation of funds awarded  
7           under this section.

8           “(f) MULTISTATE GRANTS.—

9           “(1) IN GENERAL.—The Secretary, acting  
10          through the Director, may award grants under this  
11          section to a group of two or more eligible entities to  
12          support multistate efforts to address cybersecurity  
13          risks and cybersecurity threats to information sys-  
14          tems within the jurisdictions of the eligible entities.

15          “(2) SATISFACTION OF OTHER REQUIRE-  
16          MENTS.—In order to be eligible for a multistate  
17          grant under this subsection, each eligible entity that  
18          comprises a multistate group shall submit to the  
19          Secretary—

20                 “(A) a Cybersecurity Plan for approval in  
21                 accordance with subsection (i); and

22                 “(B) a plan for establishing a cybersecu-  
23                 rity planning committee under subsection (g).

24          “(3) APPLICATION.—

1           “(A) IN GENERAL.—A multistate group  
2           applying for a multistate grant under para-  
3           graph (1) shall submit to the Secretary an ap-  
4           plication at such time, in such manner, and  
5           containing such information as the Secretary  
6           may require.

7           “(B) MULTISTATE PROJECT DESCRIP-  
8           TION.—An application of a multistate group  
9           under subparagraph (A) shall include a plan de-  
10          scribing—

11           “(i) the division of responsibilities  
12           among the eligible entities that comprise  
13           the multistate group for administering the  
14           grant for which application is being made;

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

18           “(iii) how the eligible entities that  
19           comprise the multistate group will work to-  
20           gether to implement the Cybersecurity  
21           Plan of each of those eligible entities.

22          “(g) PLANNING COMMITTEES.—

23           “(1) IN GENERAL.—An eligible entity that re-  
24           ceives a grant under this section shall establish a cy-  
25           bersecurity planning committee to—



1           “(A) assist in the development, implemen-  
2           tation, and revision of the Cybersecurity Plan of  
3           the eligible entity;

4           “(B) approve the Cybersecurity Plan of the  
5           eligible entity; and

6           “(C) assist in the determination of effec-  
7           tive funding priorities for a grant under this  
8           section in accordance with subsection (h).

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

11           “(A) be comprised of representatives from  
12           the eligible entity and counties, cities, towns,  
13           Tribes, and public educational and health insti-  
14           tutions within the jurisdiction of the eligible en-  
15           tity; and

16           “(B) include, as appropriate, representa-  
17           tives of rural, suburban, and high-population  
18           jurisdictions.

19           “(3) CYBERSECURITY EXPERTISE.—Not less  
20          than  $\frac{1}{2}$  of the representatives of a committee estab-  
21          lished under paragraph (1) shall have professional  
22          experience relating to cybersecurity or information  
23          technology.

24           “(4) RULE OF CONSTRUCTION REGARDING EX-  
25          ISTING PLANNING COMMITTEES.—Nothing in this

1 subsection may be construed to require an eligible  
2 entity to establish a cybersecurity planning com-  
3 mittee if the eligible entity has established and uses  
4 a multijurisdictional planning committee or commis-  
5 sion that meets, or may be leveraged to meet, the re-  
6 quirements of this subsection.

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

9 “(1) implement the Cybersecurity Plan of the  
10 eligible entity;

11 “(2) develop or revise the Cybersecurity Plan of  
12 the eligible entity; or

13 “(3) assist with activities that address immi-  
14 nent cybersecurity risks or cybersecurity threats to  
15 the information systems of the eligible entity or a  
16 local or Tribal organization within the jurisdiction of  
17 the eligible entity.

18 “(i) APPROVAL OF PLANS.—

19 “(1) APPROVAL AS CONDITION OF GRANT.—Be-  
20 fore an eligible entity may receive a grant under this  
21 section, the Secretary, acting through the Director,  
22 shall review the Cybersecurity Plan, or any revisions  
23 thereto, of the eligible entity and approve such plan,  
24 or revised plan, if it satisfies the requirements speci-  
25 fied in paragraph (2).

1           “(2) PLAN REQUIREMENTS.—In approving a  
2           Cybersecurity Plan of an eligible entity under this  
3           subsection, the Director shall ensure that the Cyber-  
4           security Plan—

5                   “(A) satisfies the requirements of sub-  
6                   section (e)(2);

7                   “(B) upon the issuance of the Homeland  
8                   Security Strategy to Improve the Cybersecurity  
9                   of State, Local, Tribal, and Territorial Govern-  
10                  ments authorized pursuant to section 2210(e),  
11                  complies, as appropriate, with the goals and ob-  
12                  jectives of the strategy; and

13                  “(C) has been approved by the cybersecu-  
14                  rity planning committee of the eligible entity es-  
15                  tablished under subsection (g).

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

20           “(4) EXCEPTION.—Notwithstanding subsection  
21           (e) and paragraph (1) of this subsection, the Sec-  
22           retary may award a grant under this section to an  
23           eligible entity that does not submit a Cybersecurity  
24           Plan to the Secretary if—

1           “(A) the eligible entity certifies to the Sec-  
2           retary that—

3                   “(i) the activities that will be sup-  
4                   ported by the grant are integral to the de-  
5                   velopment of the Cybersecurity Plan of the  
6                   eligible entity; and

7                   “(ii) the eligible entity will submit by  
8                   September 30, 2023, to the Secretary a  
9                   Cybersecurity Plan for review, and if ap-  
10                  propriate, approval; or

11                  “(B) the eligible entity certifies to the Sec-  
12                  retary, and the Director confirms, that the eli-  
13                  gible entity will use funds from the grant to as-  
14                  sist with the activities described in subsection  
15                  (h)(3).

16                  “(j) LIMITATIONS ON USES OF FUNDS.—

17                   “(1) IN GENERAL.—An eligible entity that re-  
18                   ceives a grant under this section may not use the  
19                   grant—

20                           “(A) to supplant State, local, or Tribal  
21                           funds;

22                           “(B) for any recipient cost-sharing con-  
23                           tribution;

24                           “(C) to pay a demand for ransom in an at-  
25                           tempt to—

1           “(i) regain access to information or  
2           an information system of the eligible entity  
3           or of a local or Tribal organization within  
4           the jurisdiction of the eligible entity; or

5           “(ii) prevent the disclosure of infor-  
6           mation that has been removed without au-  
7           thorization from an information system of  
8           the eligible entity or of a local or Tribal or-  
9           ganization within the jurisdiction of the eli-  
10          gible entity;

11          “(D) for recreational or social purposes; or

12          “(E) for any purpose that does not address  
13          cybersecurity risks or cybersecurity threats on  
14          information systems of the eligible entity or of  
15          a local or Tribal organization within the juris-  
16          diction of the eligible entity.

17          “(2) PENALTIES.—In addition to any other  
18          remedy available, the Secretary may take such ac-  
19          tions as are necessary to ensure that a recipient of  
20          a grant under this section uses the grant for the  
21          purposes for which the grant is awarded.

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

1       this section on the basis that a State, local, or Trib-  
2       al organization has previously used State, local, or  
3       Tribal funds to support the same or similar uses.

4       “(k) OPPORTUNITY TO AMEND APPLICATIONS.—In  
5       considering applications for grants under this section, the  
6       Secretary shall provide applicants with a reasonable op-  
7       portunity to correct defects, if any, in such applications  
8       before making final awards.

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

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

19           “(2) REMAINDER.—The Secretary shall appor-  
20      tion the remainder of such amounts in the ratio  
21      that—

22                   “(A) the population of each eligible entity,  
23      bears to

24                   “(B) the population of all eligible entities.

1           “(3) MINIMUM ALLOCATION TO INDIAN  
2 TRIBES.—

3           “(A) IN GENERAL.—In apportioning  
4 amounts under this section, the Secretary shall  
5 ensure that, for each fiscal year, directly eligible  
6 Tribes collectively receive, from amounts appro-  
7 priated under the State and Local Cybersecu-  
8 rity Grant Program, not less than an amount  
9 equal to three percent of the total amount ap-  
10 propriated for grants under this section.

11           “(B) ALLOCATION.—Of the amount re-  
12 served under subparagraph (A), funds shall be  
13 allocated in a manner determined by the Sec-  
14 retary in consultation with Indian tribes.

15           “(C) EXCEPTION.—This paragraph shall  
16 not apply in any fiscal year in which the Sec-  
17 retary—

18                   “(i) receives fewer than five applica-  
19 tions from Indian tribes; or

20                   “(ii) does not approve at least two ap-  
21 plication from Indian tribes.

22           “(m) FEDERAL SHARE.—

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

1 available with a grant under this section may not ex-  
2 ceed—

3 “(A) in the case of a grant to an eligible  
4 entity—

5 “(i) for fiscal year 2022, 90 percent;

6 “(ii) for fiscal year 2023, 80 percent;

7 “(iii) for fiscal year 2024, 70 percent;

8 “(iv) for fiscal year 2025, 60 percent;

9 and

10 “(v) for fiscal year 2026 and each  
11 subsequent fiscal year, 50 percent; and

12 “(B) in the case of a grant to a multistate  
13 group—

14 “(i) for fiscal year 2022, 95 percent;

15 “(ii) for fiscal year 2023, 85 percent;

16 “(iii) for fiscal year 2024, 75 percent;

17 “(iv) for fiscal year 2025, 65 percent;

18 and

19 “(v) for fiscal year 2026 and each  
20 subsequent fiscal year, 55 percent.

21 “(2) WAIVER.—The Secretary may waive or  
22 modify the requirements of paragraph (1) for an In-  
23 dian tribe if the Secretary determines such a waiver  
24 is in the public interest.

25 “(n) RESPONSIBILITIES OF GRANTEES.—



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

5                   “(A) for the purpose for which the grant  
6 is awarded; and

7                   “(B) in compliance with, as the case may  
8 be—

9                           “(i) the Cybersecurity Plan of the eli-  
10 gible entity;

11                           “(ii) the Cybersecurity Plans of the el-  
12 igible entities that comprise the multistate  
13 group; or

14                           “(iii) a purpose approved by the Sec-  
15 retary under subsection (h) or pursuant to  
16 an exception under subsection (i).

17           “(2) AVAILABILITY OF FUNDS TO LOCAL AND  
18 TRIBAL ORGANIZATIONS.—Not later than 45 days  
19 after the date on which an eligible entity or  
20 multistate group receives a grant under this section,  
21 the eligible entity or multistate group shall, without  
22 imposing unreasonable or unduly burdensome re-  
23 quirements as a condition of receipt, obligate or oth-  
24 erwise make available to local and Tribal organiza-  
25 tions within the jurisdiction of the eligible entity or

1 the eligible entities that comprise the multistate  
2 group, and as applicable, consistent with the Cyber-  
3 security Plan of the eligible entity or the Cybersecu-  
4 rity Plans of the eligible entities that comprise the  
5 multistate group—

6 “(A) not less than 80 percent of funds  
7 available under the grant;

8 “(B) with the consent of the local and  
9 Tribal organizations, items, services, capabili-  
10 ties, or activities having a value of not less than  
11 80 percent of the amount of the grant; or

12 “(C) with the consent of the local and  
13 Tribal organizations, grant funds combined  
14 with other items, services, capabilities, or activi-  
15 ties having the total value of not less than 80  
16 percent of the amount of the grant.

17 “(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL AND TRIBAL OR-  
18 GANIZATIONS.—An eligible entity or multistate  
19 group shall certify to the Secretary that the eligible  
20 entity or multistate group has made the distribution  
21 to local, Tribal, and territorial governments required  
22 under paragraph (2).  
23

24 “(4) EXTENSION OF PERIOD.—

1           “(A) IN GENERAL.—An eligible entity or  
2           multistate group may request in writing that  
3           the Secretary extend the period of time speci-  
4           fied in paragraph (2) for an additional period  
5           of time.

6           “(B) APPROVAL.—The Secretary may ap-  
7           prove a request for an extension under subpara-  
8           graph (A) if the Secretary determines the ex-  
9           tension is necessary to ensure that the obliga-  
10          tion and expenditure of grant funds align with  
11          the purpose of the State and Local Cybersecu-  
12          rity Grant Program.

13          “(5) EXCEPTION.—Paragraph (2) shall not  
14          apply to the District of Columbia, the Common-  
15          wealth of Puerto Rico, American Samoa, the Com-  
16          monwealth of the Northern Mariana Islands, Guam,  
17          the Virgin Islands, or an Indian tribe.

18          “(6) DIRECT FUNDING.—If an eligible entity  
19          does not make a distribution to a local or Tribal or-  
20          ganization required in accordance with paragraph  
21          (2), the local or Tribal organization may petition the  
22          Secretary to request that grant funds be provided di-  
23          rectly to the local or Tribal organization.

24          “(7) PENALTIES.—In addition to other rem-  
25          edies available to the Secretary, the Secretary may

1 terminate or reduce the amount of a grant awarded  
2 under this section to an eligible entity or distribute  
3 grant funds previously awarded to such eligible enti-  
4 ty directly to the appropriate local or Tribal organi-  
5 zation as a replacement grant in an amount the Sec-  
6 retary determines appropriate if such eligible entity  
7 violates a requirement of this subsection.

8 “(o) ADVISORY COMMITTEE.—

9 “(1) ESTABLISHMENT.—Not later than 120  
10 days after the date of enactment of this section, the  
11 Director shall establish a State and Local Cyberse-  
12 curity Resilience Committee to provide State, local,  
13 and Tribal stakeholder expertise, situational aware-  
14 ness, and recommendations to the Director, as ap-  
15 propriate, regarding how to—

16 “(A) address cybersecurity risks and cyber-  
17 security threats to information systems of  
18 State, local, or Tribal organizations; and

19 “(B) improve the ability of State, local,  
20 and Tribal organizations to prevent, protect  
21 against, respond to, mitigate, and recover from  
22 such cybersecurity risks and cybersecurity  
23 threats.

24 “(2) DUTIES.—The committee established  
25 under paragraph (1) shall—

1           “(A) submit to the Director recommenda-  
2           tions that may inform guidance for applicants  
3           for grants under this section;

4           “(B) upon the request of the Director, pro-  
5           vide to the Director technical assistance to in-  
6           form the review of Cybersecurity Plans sub-  
7           mitted by applicants for grants under this sec-  
8           tion, and, as appropriate, submit to the Direc-  
9           tor recommendations to improve those plans  
10          prior to the approval of the plans under sub-  
11          section (i);

12          “(C) advise and provide to the Director  
13          input regarding the Homeland Security Strat-  
14          egy to Improve Cybersecurity for State, Local,  
15          Tribal, and Territorial Governments required  
16          under section 2210;

17          “(D) upon the request of the Director, pro-  
18          vide to the Director recommendations, as ap-  
19          propriate, regarding how to—

20                  “(i) address cybersecurity risks and  
21                  cybersecurity threats on information sys-  
22                  tems of State, local, or Tribal organiza-  
23                  tions; and

1                   “(ii) improve the cybersecurity resil-  
2                   ience of State, local, or Tribal organiza-  
3                   tions; and

4                   “(E) regularly coordinate with the State,  
5                   Local, Tribal and Territorial Government Co-  
6                   ordinating Council, within the Critical Infra-  
7                   structure Partnership Advisory Council, estab-  
8                   lished under section 871.

9                   “(3) MEMBERSHIP.—

10                   “(A) NUMBER AND APPOINTMENT.—The  
11                   State and Local Cybersecurity Resilience Com-  
12                   mittee established pursuant to paragraph (1)  
13                   shall be composed of 15 members appointed by  
14                   the Director, as follows:

15                   “(i) Two individuals recommended to  
16                   the Director by the National Governors As-  
17                   sociation.

18                   “(ii) Two individuals recommended to  
19                   the Director by the National Association of  
20                   State Chief Information Officers.

21                   “(iii) One individual recommended to  
22                   the Director by the National Guard Bu-  
23                   reau.

1                   “(iv) Two individuals recommended to  
2                   the Director by the National Association of  
3                   Counties.

4                   “(v) One individual recommended to  
5                   the Director by the National League of  
6                   Cities.

7                   “(vi) One individual recommended to  
8                   the Director by the United States Con-  
9                   ference of Mayors.

10                  “(vii) One individual recommended to  
11                  the Director by the Multi-State Informa-  
12                  tion Sharing and Analysis Center.

13                  “(viii) One individual recommended to  
14                  the Director by the National Congress of  
15                  American Indians.

16                  “(viii) Four individuals who have edu-  
17                  cational and professional experience relat-  
18                  ing to cybersecurity work or cybersecurity  
19                  policy.

20                  “(B) TERMS.—

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

1           “(ii) REQUIREMENT.—At least two  
2 members of the State and Local Cyberse-  
3 curity Resilience Committee shall also be  
4 members of the State, Local, Tribal and  
5 Territorial Government Coordinating  
6 Council, within the Critical Infrastructure  
7 Partnership Advisory Council, established  
8 under section 871.

9           “(iii) EXCEPTION.—A term of a mem-  
10 ber of the State and Local Cybersecurity  
11 Resilience Committee shall be three years  
12 if the member is appointed initially to the  
13 Committee upon the establishment of the  
14 Committee.

15           “(iv) TERM REMAINDERS.—Any mem-  
16 ber of the State and Local Cybersecurity  
17 Resilience Committee appointed to fill a  
18 vacancy occurring before the expiration of  
19 the term for which the member’s prede-  
20 cessor was appointed shall be appointed  
21 only for the remainder of such term. A  
22 member may serve after the expiration of  
23 such member’s term until a successor has  
24 taken office.



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

5                   “(C) PAY.—Members of the State and  
6                   Local Cybersecurity Resilience Committee shall  
7                   serve without pay.

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

12                  “(5) PERMANENT AUTHORITY.—Notwith-  
13                  standing section 14 of the Federal Advisory Com-  
14                  mittee Act (5 U.S.C. App.), the State and Local Cy-  
15                  bersecurity Resilience Committee shall be a perma-  
16                  nent authority.

17                  “(p) REPORTS.—

18                  “(1) ANNUAL REPORTS BY GRANT RECIPI-  
19                  ENTS.—

20                  “(A) IN GENERAL.—Not later than one  
21                  year after an eligible entity or multistate group  
22                  receives funds under this section, the eligible  
23                  entity or multistate group shall submit to the  
24                  Secretary a report on the progress of the eligi-  
25                  ble entity or multistate group in implementing

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

5 “(B) ABSENCE OF PLAN.—Not later than  
6 180 days after an eligible entity that does not  
7 have a Cybersecurity Plan receives funds under  
8 this section for developing its Cybersecurity  
9 Plan, the eligible entity shall submit to the Sec-  
10 retary a report describing how the eligible enti-  
11 ty obligated and expended grant funds during  
12 the fiscal year to—

13 “(i) so develop such a Cybersecurity  
14 Plan; or

15 “(ii) assist with the activities de-  
16 scribed in subsection (h)(3).

17 “(2) ANNUAL REPORTS TO CONGRESS.—Not  
18 less frequently than once per year, the Secretary,  
19 acting through the Director, shall submit to Con-  
20 gress a report on the use of grants awarded under  
21 this section and any progress made toward the fol-  
22 lowing:

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

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

3           “(B) Developing, implementing, or revising  
4           Cybersecurity Plans.

5           “(C) Reducing cybersecurity risks and cy-  
6           bersecurity threats to information systems, ap-  
7           plications, and user accounts owned or operated  
8           by or on behalf of State, local, and Tribal orga-  
9           nizations as a result of the award of such  
10          grants.

11          “(q) AUTHORIZATION OF APPROPRIATIONS.—There  
12          are authorized to be appropriated for grants under this  
13          section—

14                 “(1) for each of fiscal years 2022 through  
15                 2026, \$500,000,000; and

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

18          **“SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOP-**  
19                         **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**  
20                         **RITORIAL GOVERNMENT OFFICIALS.**

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

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

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

“Sec. 2220A. State and Local Cybersecurity Grant Program.

“Sec. 2220B. Cybersecurity resource guide development for State, local, Tribal,  
and territorial government officials.”.

9 **SEC. 3. STRATEGY.**

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

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

18 “(1) IN GENERAL.—

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

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

7 “(B) RECOMMENDATIONS AND REQUIRE-  
8 MENTS.—The strategy required under subpara-  
9 graph (A) shall—

10 “(i) provide recommendations relating  
11 to the ways in which the Federal Govern-  
12 ment should support and promote the abil-  
13 ity of State, local, Tribal, and territorial  
14 governments to identify, mitigate against,  
15 protect against, detect, respond to, and re-  
16 cover from cybersecurity risks (as such  
17 term is defined in section 2209), cyberse-  
18 curity threats, and incidents (as such term  
19 is defined in section 2209); and

20 “(ii) establish baseline requirements  
21 for cybersecurity plans under this section  
22 and principles with which such plans shall  
23 align.

24 “(2) CONTENTS.—The strategy required under  
25 paragraph (1) shall—

1           “(A) identify capability gaps in the ability  
2 of State, local, Tribal, and territorial govern-  
3 ments to identify, protect against, detect, re-  
4 spond to, and recover from cybersecurity risks,  
5 cybersecurity threats, incidents, and  
6 ransomware incidents;

7           “(B) identify Federal resources and capa-  
8 bilities that are available or could be made  
9 available to State, local, Tribal, and territorial  
10 governments to help those governments identify,  
11 protect against, detect, respond to, and recover  
12 from cybersecurity risks, cybersecurity threats,  
13 incidents, and ransomware incidents;

14           “(C) identify and assess the limitations of  
15 Federal resources and capabilities available to  
16 State, local, Tribal, and territorial governments  
17 to help those governments identify, protect  
18 against, detect, respond to, and recover from  
19 cybersecurity risks, cybersecurity threats, inci-  
20 dents, and ransomware incidents and make rec-  
21 ommendations to address such limitations;

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

1 Information Sharing and Analysis Center, to  
2 improve—

3 “(i) incident exercises, information  
4 sharing and incident notification proce-  
5 dures;

6 “(ii) the ability for State, local, Trib-  
7 al, and territorial governments to volun-  
8 tarily adapt and implement guidance in  
9 Federal binding operational directives; and

10 “(iii) opportunities to leverage Federal  
11 schedules for cybersecurity investments  
12 under section 502 of title 40, United  
13 States Code;

14 “(E) recommend new initiatives the Fed-  
15 eral Government should undertake to improve  
16 the ability of State, local, Tribal, and territorial  
17 governments to identify, protect against, detect,  
18 respond to, and recover from cybersecurity  
19 risks, cybersecurity threats, incidents, and  
20 ransomware incidents;

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

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

3 “(G) set dates, including interim bench-  
4 marks, as appropriate for State, local, Tribal,  
5 and territorial governments to establish baseline  
6 capabilities to identify, protect against, detect,  
7 respond to, and recover from cybersecurity  
8 risks, cybersecurity threats, incidents, and  
9 ransomware incidents.

10 “(3) CONSIDERATIONS.—In developing the  
11 strategy required under paragraph (1), the Director,  
12 in coordination with the heads of appropriate Fed-  
13 eral agencies, State, local, Tribal, and territorial  
14 governments, the State and Local Cybersecurity Re-  
15 siliency Committee established under section 2220A,  
16 and other stakeholders, as appropriate, shall con-  
17 sider—

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

22 “(B) the impact of incidents that have af-  
23 fected State, local, Tribal, and territorial gov-  
24 ernments, including the resulting costs to such  
25 governments;



1           “(C) the information related to the interest  
2           and ability of state and non-state threat actors  
3           to compromise information systems (as such  
4           term is defined in section 102 of the Cybersecu-  
5           rity Act of 2015 (6 U.S.C. 1501)) owned or op-  
6           erated by State, local, Tribal, and territorial  
7           governments;

8           “(D) emerging cybersecurity risks and cy-  
9           bersecurity threats to State, local, Tribal, and  
10          territorial governments resulting from the de-  
11          ployment of new technologies; and

12          “(E) recommendations made by the State  
13          and Local Cybersecurity Resilience Committee  
14          established under section 2220A.

15          “(4) EXEMPTION.—Chapter 35 of title 44,  
16          United States Code (commonly known as the ‘Paper-  
17          work Reduction Act’), shall not apply to any action  
18          to implement this subsection.”.

19          (b) RESPONSIBILITIES OF THE DIRECTOR OF THE  
20          CYBERSECURITY AND INFRASTRUCTURE SECURITY AGEN-  
21          CY.—Section 2202 of the Homeland Security Act of 2002  
22          (6 U.S.C. 652) is amended—

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

1           (2) by inserting after subsection (c) the fol-  
2           lowing new subsection:

3           “(d) **ADDITIONAL RESPONSIBILITIES.**—In addition  
4 to the responsibilities under subsection (c), the Director  
5 shall—

6           “(1) develop program guidance, in consultation  
7 with the State and Local Government Cybersecurity  
8 Resilience Committee established under section  
9 2220A, for the State and Local Cybersecurity Grant  
10 Program under such section or any other homeland  
11 security assistance administered by the Department  
12 to improve cybersecurity;

13           “(2) review, in consultation with the State and  
14 Local Cybersecurity Resilience Committee, all cyber-  
15 security plans of State, local, Tribal, and territorial  
16 governments developed pursuant to any homeland  
17 security assistance administered by the Department  
18 to improve cybersecurity;

19           “(3) provide expertise and technical assistance  
20 to State, local, Tribal, and territorial government of-  
21 ficials with respect to cybersecurity; and

22           “(4) provide education, training, and capacity  
23 development to enhance the security and resilience  
24 of cybersecurity and infrastructure security.”.

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

9 **SEC. 4. TITLE XXII TECHNICAL AND CLERICAL AMEND-**  
10 **MENTS.**

11 (a) TECHNICAL AMENDMENTS.—

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

15 (A) in the first section 2215 (6 U.S.C.  
16 665; relating to the duties and authorities relat-  
17 ing to .gov internet domain), by amending the  
18 section enumerator and heading to read as fol-  
19 lows:

20 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**  
21 **INTERNET DOMAIN.”;**

22 (B) in the second section 2215 (6 U.S.C.  
23 665b; relating to the joint cyber planning of-  
24 fice), by amending the section enumerator and  
25 heading to read as follows:

1 **“SEC. 2216. JOINT CYBER PLANNING OFFICE.”;**

2 (C) in the third section 2215 (6 U.S.C.  
3 665c; relating to the Cybersecurity State Coor-  
4 dinator), by amending the section enumerator  
5 and heading to read as follows:

6 **“SEC. 2217. CYBERSECURITY STATE COORDINATOR.”;**

7 (D) in the fourth section 2215 (6 U.S.C.  
8 665d; relating to Sector Risk Management  
9 Agencies), by amending the section enumerator  
10 and heading to read as follows:

11 **“SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.”;**

12 (E) in section 2216 (6 U.S.C. 665e; relat-  
13 ing to the Cybersecurity Advisory Committee),  
14 by amending the section enumerator and head-  
15 ing to read as follows:

16 **“SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.”; and**

17 (F) in section 2217 (6 U.S.C. 665f; relat-  
18 ing to Cybersecurity Education and Training  
19 Programs), by amending the section enu-  
20 merator and heading to read as follows:

21 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**  
22 **PROGRAMS.”.**

23 (2) CONSOLIDATED APPROPRIATIONS ACT,  
24 2021.—Paragraph (1) of section 904(b) of division U  
25 of the Consolidated Appropriations Act, 2021 (Pub-  
26 lic Law 116–260) is amended, in the matter pre-

1 ceding subparagraph (A), by inserting “of 2002”  
2 after “Homeland Security Act”.

3 (b) CLERICAL AMENDMENT.—The table of contents  
4 in section 1(b) of the Homeland Security Act of 2002 is  
5 amended by striking the items relating to sections 2214  
6 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:

1           “(6) Supporting the development and imple-  
2           mentation of a security directive or regulation when  
3           the Administrator issues such a directive or regula-  
4           tion.”.

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:

1       (c) CYBERSECURITY EXPERTISE.—The strategy shall  
2 include an assessment of the cybersecurity expertise deter-  
3 mined necessary by the Administrator of the Transpor-  
4 tation Security Administration and a plan for developing  
5 such expertise within the Administration.

