with you on this legislation and other matters of great importance to this Nation.

Sincerely,

BENNIE G. THOMPSON,
Chairman,
Committee on Homeland Security.

Mr. GUEST. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 2795, the DHS Blue Campaign Enhancement Act. As vice-ranking member of the Homeland Security Committee, I know how important it is for us to approach protecting this great Nation in a comprehensive manner by tackling all types of threats, including: hackers, terrorists, violent criminals, and human traffickers.

Criminal organizations use human trafficking to fund their operations by defrauding, coercing, and exploiting both adults and children, forcing them into labor and commercial sex acts. The DHS Blue Campaign enables and empowers the DHS workforce and customer-facing industries they work with—industries such as airlines—to recognize the indicators of human trafficking and take the proper steps to alert authorities.

H.R. 2795 enhances the Department's existing training opportunities by developing internet-based training programs to train Federal, State, local, Tribal law enforcement officers, and others as part of the Department's Blue Campaign. This important piece of legislation also established the Blue Campaign Advisory Board within the Department to coordinate Blue Campaign efforts and work cohesively to combat human trafficking.

Empowering State and local law enforcement to recognize potential human trafficking is the first step in helping them assist these victims, many of whom have been told that they have broken the law and can't seek police assistance by their traffickers. H.R. 2795 does this and helps disrupt these criminal networks, which is an important component in dismantling criminals and the terrorists financing their acts around the world.

I want to thank Representative MEIJER for his leadership, and Chairman THOMPSON for moving this legislation out of committee, and I urge my colleagues to support this important bill to further secure the homeland.

Madam Speaker, I reserve the balance of my time.

Ms. BARRAGÁN. Madam Speaker, I have no more speakers, and I am prepared to close after the gentleman from Mississippi closes. I reserve the balance of my time.

Mr. GUEST. Madam Speaker, I yield 2 minutes to the gentleman from Michigan (Mr. MEIJER).

Mr. MEIJER. Madam Speaker, I rise in support of H.R. 2795, the DHS Blue Campaign Enhancement Act. This bill, which I am proud to have introduced with my colleague, the chairman of the Homeland Security Subcommittee on Oversight, Management, and Accountability, Representative CORREA, has one very specific goal, to combat human trafficking.

According to the Department of State's Trafficking in Persons Report, every year, around the world tens of thousands of men, women, and children are trafficked, including far too many right here in the United States. Human traffickers use fraud and coercion to compel people into situations of forced labor or sexual exploitation. False promises of well-paying jobs, romantic relationships, and violence are all methods used by human traffickers. Victims can be any age, race, gender, or nationality and from any socioeconomic background.

To curb this horrific practice, we must use a multipronged approach, and a critical component to this strategy is ensuring that law enforcement personnel and employees in customer-facing industries are trained to identify a potential victim of human trafficking by recognizing key indicators and taking appropriate action.

DHS started the Blue Campaign in 2010 to do just that; to unify and coordinate Department efforts to address human trafficking. The Blue Campaign enables and empowers the DHS workforce and the industries they work with—including airlines and the public—to recognize the indicators of human trafficking and take steps to alert the appropriate authorities.

My bill, the DHS Blue Campaign Enhancement Act, bolsters these efforts by creating an advisory board to inform and coordinate training among the DHS components to increase the efficiency and effectiveness of the training that DHS provides for its personnel, its industries, and State and local law enforcement partners.

This legislation also increases the online trainings that DHS will provide, enabling the Department to reach a broader audience more quickly.

I would like to thank my good friend from California (Mr. CORREA) for joining me in this effort and supporting this important piece of legislation.

Madam Speaker, I urge my colleagues to approve this bill and help DHS do its part to combat human trafficking.

Mr. GUEST. Madam Speaker, I have no further speakers, and I urge Members to support this bill.

Madam Speaker, I yield back the balance of my time.

Ms. BARRAGÁN. Madam Speaker, I yield myself the balance of my time.

Madam Speaker, DHS is uniquely positioned to address human trafficking through the Blue Campaign. H.R. 2795 seeks to build upon the success of the Blue Campaign, which was first established in August 2010, and to bolster human trafficking awareness by ensuring that public-facing materials remain as current and accessible as possible. This is a worthwhile endeavor.

Madam Speaker, I urge passage of the bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from California (Ms. BARRAGÁN) that the House suspend the rules and pass the bill, H.R. 2795, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. MOORE of Alabama. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

□ 1300

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 3138) to amend the Homeland Security Act of 2002 to authorize a grant program relating to the cybersecurity of State and local governments, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3138

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''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.

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

''(11) 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 eligible 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 applications 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 Territorial 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, 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).''.

(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 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.''.

The SPEAKER pro tempore (Ms. KAPTUR). Pursuant to the rule, the gentlewoman from New York (Ms. CLARKE) and the gentleman from Mississippi (Mr. GUEST) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Ms. CLARKE of New York. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from New York?

There was no objection.

Ms. CLARKE of New York. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, the recent Colonial Pipeline, JBS, and Kaseya ransomware attacks have brought the Nation's attention to the tremendous national security threat posed by ransomware.

The Colonial Pipeline breach alone disrupted the supply of gasoline for a

large portion of the Nation and contributed to gas shortages across much of the Southeast. It also spurred conversations about how much of our Nation's critical infrastructure is privately owned and operated.

Lost on many Americans is how much vulnerable critical infrastructure is actually in the public sector. Today, emergency services, public schools, hospitals, and agencies involved in providing essential services or regulating important industries are all housed in our State and local governments. In recent years, we have seen communities, big and small, that lacked dedicated cybersecurity resources fall victim to ransomware attacks.

The types of incidents we have seen include a ransomware attack on Baltimore that cost city taxpayers $18 million; a hack on the D.C. police department that resulted in leaked sensitive personnel files; and a cyberattack against a Massachusetts school district that forced it to cancel its first day of in-person instruction earlier this year.

In May, my subcommittee held a hearing on the ransomware crisis where experts shared their views on the policy solutions that the Federal Government can consider to address this challenge. Our witnesses uniformly urged greater investment in prevention, particularly at the State and local levels.

We cannot just focus on responding to cyber incidents. We must help our communities reduce their vulnerability and better mitigate incidents when they occur.

In the long term, front-end cybersecurity investments save money, protect infrastructure, and prevent disruption to our economy and in our communities.

That is why I introduced the State and Local Cybersecurity Improvement Act. It authorizes $500 million annually for grants to State, local, territorial, and Tribal governments to upgrade their cybersecurity. It requires States to pay a graduated cost share to incentivize them to budget better for cybersecurity, and it requires them to develop cybersecurity plans so we ensure these funds are well-spent.

My bill also requires DHS to create a plan to improve the cybersecurity posture of State and local governments to ensure that States have goals and objectives to which they align their own cybersecurity plans.

We have spent considerable resources enhancing the security of our Federal networks, and President Biden's recent executive order, along with investments included in the American Rescue Plan, demonstrate a continued commitment to strengthening Federal cybersecurity.

These actions are incredibly important, but we need to do more to address the vulnerabilities at the State and local levels, where there has been inadequate investment in cybersecurity for years.

It is essential for the Federal Government to be a partner in protecting State and local digital infrastructure. As Congress considers ways to invest in our Nation's infrastructure, State and local digital infrastructure must be a part of that conversation.

As we have seen in recent months, the gap between the digital world and the physical one is smaller than ever. I appreciate the bipartisan recognition of that and the strong support this investment in our infrastructure security received in the Homeland Security Committee.

In particular, I want to thank Chairman THOMPSON, Ranking Member KATKO, Ranking Member GARBARINO, and Representatives MCCAUL, RUPPERSBERGER, KILMER, and SLOTKIN for cosponsoring this legislation.

By passing the State and Local Cybersecurity Improvement Act today, we can demonstrate to the American people that Congress can work in a bipartisan way to make a meaningful difference in addressing our Nation's cybersecurity risk.

Madam Speaker, I urge all of my colleagues to support this important bill, and I reserve the balance of my time.

Mr. GUEST. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 3138, the State and Local Cybersecurity Improvement Act of 2021.

I thank Chairwoman CLARKE, Chairman THOMPSON, Ranking Member GARBARINO, and my other committee colleagues for their leadership on H.R. 3138.

Over the past year, we have seen the devastating impact a ransomware attack can have on our Nation's most critical infrastructure. But we must not forget that no one is immune from cyber criminals, including our State and local governments.

I am pleased today that the House is taking action to give our State and local partners, and CISA, a leg up against these cyber criminals.

This bill will have a tremendous impact on the cybersecurity posture of State and local governments by focusing important funding and expertise on the front lines, the State and local levels.

I urge all Members to join me in supporting H.R. 3138, and I reserve the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield 2 minutes to the gentlewoman from Texas (Ms. JACKSON LEE).

Ms. JACKSON LEE. Madam Speaker, I thank the gentlewoman from New York for her leadership on the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.

Madam Speaker, I rise to support the State and Local Cybersecurity Improvement Act.

I particularly emphasize the fact that we are the United States of America, but the cyberattacks occur in our neighborhoods, our hamlets, our cities, our counties, and our States. They occur right under our noses, and they impact our constituents by taking their personal records from the Texas Medical Center, for example, impacting the medical care of people, interfering with various diagnostic machines, and dealing with the energy infrastructure, such as the Colonial Pipeline incident. These are happening in our neighborhoods.

The State and Local Cybersecurity Improvement Act will make $500 million available in grants from the Department of Homeland Security to State, local, and Tribal entities over the next 4 years as they address critical cybersecurity risks facing information systems.

I will soon rise to the floor on legislation that I have authored, and I will make this point, Madam Speaker: It is crucial that the other body begins to address the legislation that this House is able to pass because we are passing innovative, corrective, and needed legislation.

Cyber is not a joke, if I can say that. Neither are the attacks on our cyber infrastructure.

However, the Department of Homeland Security was created in 2002 to bring together the expertise of several different government entities to protect against foreign threats. At that time, the Nation's main concern was protecting our citizens and residents from another large-scale terrorist attack, one that we had never seen before: attacking tall buildings with airplanes. We had never seen it.

But, today, 2021, is not 2001. It is not 20 years ago, and the landscape of terrorism has changed enormously. With rapid advancement in technology and malign foreign cyber aggression in nation-states that are not engaged, this bill is important.

Madam Speaker, I ask my colleagues to support this bipartisan legislation, H.R. 3138, that will provide us a way to address this issue.

Mr. GUEST. Madam Speaker, I urge Members to support this bill, and I yield back the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield myself the balance of my time.

Madam Speaker, while cybersecurity threats are not new, this year has highlighted the serious impact cyber incidents can have on our national security.

The United States has as much cybersecurity expertise as any country. But without adequate resources, State and local governments cannot implement the policies and practices we know will make their digital infrastructure more secure.

Enactment of the State and Local Cybersecurity Improvement Act will ensure that they have the funding, planning, and support to adequately invest in securing government networks and reducing risk.

Madam Speaker, I urge my colleagues to support H.R. 3138, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by

the gentlewoman from New York (Ms. CLARKE) that the House suspend the rules and pass the bill, H.R. 3138, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. BISHOP of North Carolina. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

DHS INDUSTRIAL CONTROL SYSTEMS CAPABILITIES ENHANCEMENT ACT OF 2021

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 1833) to amend the Homeland Security Act of 2002 to provide for the responsibility of the Cybersecurity and Infrastructure Security Agency to maintain capabilities to identify threats to industrial control systems, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1833

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''DHS Industrial Control Systems Capabilities Enhancement Act of 2021''.

SEC. 2. CAPABILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

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

(1) in subsection (e)(1)—

(A) in subparagraph (G), by striking ''and'' after the semicolon;

(B) in subparagraph (H), by inserting ''and'' after the semicolon; and

(C) by adding at the end the following new subparagraph:

''(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;''; and

(2) by adding at the end the following new subsection:

''(p) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

''(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

''(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

''(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

''(5) conduct such other efforts and assistance as the Secretary determines appropriate.''.

(b) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act and every six months thereafter during the subsequent 4-year period, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the industrial control systems capabilities of the Agency under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a).

(c) GAO REVIEW.—Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall review implementation of the requirements of subsections (e)(1)(I) and (p) of section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a), and submit to the Committee on Homeland Security in the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate a report containing findings and recommendations relating to such implementation. Such report shall include information on the following:

(1) Any interagency coordination challenges to the ability of the Director of the Cybersecurity and Infrastructure Agency of the Department of Homeland Security to lead Federal efforts to identify and mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(1) of such section.

(2) The degree to which the Agency has adequate capacity, expertise, and resources to carry out threat hunting and incident response capabilities to mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(2) of such section, as well as additional resources that would be needed to close any operational gaps in such capabilities.

(3) The extent to which industrial control system stakeholders sought cybersecurity technical assistance from the Agency pursuant to subsection (p)(3) of such section, and the utility and effectiveness of such technical assistance.

(4) The degree to which the Agency works with security researchers and other industrial control systems stakeholders, pursuant to subsection (p)(4) of such section, to provide vulnerability information to the industrial control systems community.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Ms. CLARKE) and the gentleman from New York (Mr. KATKO) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Ms. CLARKE of New York. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from New York?

There was no objection.

Ms. CLARKE of New York. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in support of H.R. 1833, the DHS Industrial Control Systems Capabilities Enhancement Act.

This bill seeks to give the Cybersecurity and Infrastructure Security Agency, or CISA, a stronger hand in securing industrial control systems and would help to clarify its central coordination role across the Federal Government.

□ 1315

The importance of securing industrial control systems cannot be overstated. We rely on these systems to provide vital services, like water treatment, energy distribution, and critical manufacturing.

As control systems have grown more and more connected to business and IT networks that rely on the internet, we have seen systems become more vulnerable to cyberattacks.

Industrial control systems have been targeted by groups closely aligned with nation-states like China and Russia who seek to undermine the United States and advance their own geopolitical interests.

We have also seen criminal groups, like the perpetrators of the ransomware attack on the Colonial Pipeline, create great economic disruption while extorting companies.

It doesn't take a criminal mastermind to infiltrate an industrial environment, either. Earlier this year, an unsophisticated, unknown perpetrator was able to breach a water treatment plant in Oldsmar, Florida, and manipulate chemical levels in ways that could have poisoned nearby residents.

H.R. 1833 will strengthen CISA's authority as the lead Federal coordinator for securing industrial control systems and empower CISA to hunt for threats, respond to incidents, and to promote strong cybersecurity for critical infrastructure.

The Department of Homeland Security has been working on control system security since 2004. H.R. 1833 recognizes that role at a pivotal time as cyber threats to critical infrastructure reach new heights.

Importantly, this bill also includes a GAO review of whether CISA has the resources, staffing, and authorities it needs to effectively implement these provisions. Such oversight will be key, given that these systems are complex, diverse, and there are a limited number of skilled cyber experts capable of securing them.

Madam Speaker, I urge my colleagues to support H.R. 1833, and I reserve the balance of my time.

Mr. KATKO. Madam Speaker, I yield myself such time as I may consume.

I want to thank my colleague from New York for supporting my bill, H.R.