and the new technology that goes with it.

I think it really makes no sense to simply say we are going to wipe away these efficiency standards for laundry machines. We have had similar bills on refrigerators and other appliances because what we are all about in this country is using technology to make things more efficient, make things cheaper, and make things better for the future.

That is essentially why I oppose the bill and would ask my colleagues to vote ''no'' on this legislation.

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

Mr. DUNCAN. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, in closing, I think the difference between the Republican Party and administration and Democrats comes down to government mandating certain choices and Republicans believing in free markets, market choices, and market opportunities.

If Americans want to buy something that, in their mind, is more efficient and that can save them money, maybe will last longer, that is up to the Americans. The market will step up and provide those opportunities and products. If you want an electric vehicle, the market is going to provide that. It shouldn't be mandated.

I thank my colleague from Tennessee (Mr. OGLES) for approaching this bill that is dealing with washing machines, but the broader picture is the mandates from the administration to tell Americans the only choices they have aren't going to save them that much money in the long run, as we pointed out.

Mr. Speaker, I urge my colleagues to vote ''no'' on the motion to recommit and vote in favor of this legislation, H.R. 7673.

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

The SPEAKER pro tempore. All time for debate has expired.

Pursuant to House Resolution 1612, the previous question is ordered on the bill.

The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed and read a third time, and was read the third time.

The SPEAKER pro tempore. The question is on passage of the bill.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. PALLONE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this question will be postponed.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or votes objected to under clause 6 of rule XX.

The House will resume proceedings on postponed questions at a later time.

STRENGTHENING CYBER RESILIENCE AGAINST STATE-SPONSORED THREATS ACT

Mr. GREEN of Tennessee. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 9769) to ensure the security and integrity of United States critical infrastructure by establishing an interagency task force and requiring a comprehensive report on the targeting of United States critical infrastructure by People's Republic of China state-sponsored cyber actors, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 9769

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 ''Strengthening Cyber Resilience Against State-Sponsored Threats Act''.

SEC. 2. INTERAGENCY TASK FORCE AND REPORT ON THE TARGETING OF UNITED STATES CRITICAL INFRASTRUCTURE BY PEOPLE'S REPUBLIC OF CHINA STATE-SPONSORED CYBER ACTORS.

(a) INTERAGENCY TASK FORCE.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, in consultation with the Attorney General, the Director of the Federal Bureau of Investigation, and the heads of appropriate Sector Risk Management Agencies as determined by the Director of CISA, shall establish a joint interagency task force (in this section referred to as the ''task force'') to facilitate collaboration and coordination among the Sector Risk Management Agencies assigned a Federal role or responsibility in National Security Memorandum–22, issued April 30, 2024 (relating to critical infrastructure security and resilience), or any successor document, to detect, analyze, and respond to the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China by ensuring that such agencies' actions are aligned and mutually reinforcing.

(b) CHAIRS.—

(1) CHAIRPERSON.—The Director of CISA (or the Director of CISA's designee) shall serve as the chairperson of the task force.

(2) VICE CHAIRPERSON.—The Director of the Federal Bureau of Investigation (or such Director's designee) shall serve as the vice chairperson of the task force.

(c) COMPOSITION.—

(1) IN GENERAL.—The task force shall consist of appropriate representatives of the departments and agencies specified in subsection (a).

(2) QUALIFICATIONS.—To materially assist in the activities of the task force, representatives under paragraph (1) should be subject matter experts who have familiarity and technical expertise regarding cybersecurity, digital forensics, or threat intelligence analysis, or in-depth knowledge of the tactics, techniques, and procedures (TTPs) commonly used by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(d) VACANCY.—Any vacancy occurring in the membership of the task force shall be filled in the same manner in which the original appointment was made.

(e) ESTABLISHMENT FLEXIBILITY.—To avoid redundancy, the task force may coordinate with any preexisting task force, working group, or cross-intelligence effort within the Homeland Security Enterprise or the intelligence community that has examined or responded to the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(f) TASK FORCE REPORTS; BRIEFING.—

(1) INITIAL REPORT.—Not later than 540 days after the establishment of the task force, the task force shall submit to the appropriate congressional committees the first report containing the initial findings, conclusions, and recommendations of the task force.

(2) ANNUAL REPORT.—Not later than one year after the date of the submission of the initial report under paragraph (1) and annually thereafter for five years, the task force shall submit to the appropriate congressional committees an annual report containing the findings, conclusions, and recommendations of the task force.

(3) CONTENTS.—The reports under this subsection shall include the following:

(A) An assessment at the lowest classification feasible of the sector-specific risks, trends relating to incidents impacting sectors, and tactics, techniques, and procedures utilized by or relating to State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(B) An assessment of additional resources and authorities needed by Federal departments and agencies to better counter the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(C) A classified assessment of the extent of potential destruction, compromise, or disruption to United States critical infrastructure by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China in the event of a major crisis or future conflict between the People's Republic of China and the United States.

(D) A classified assessment of the ability of the United States to counter the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China in the event of a major crisis or future conflict between the People's Republic of China and the United States, including with respect to different cybersecurity measures and recommendations that could mitigate such a threat.

(E) A classified assessment of the ability of State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China to disrupt operations of the United States Armed Forces by hindering mobility across critical infrastructure such as rail, aviation, and ports, including how such would impair the ability of the United States Armed Forces to deploy and maneuver forces effectively.

(F) A classified assessment of the economic and social ramifications of a disruption to one or multiple United States critical infrastructure sectors by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China in the event of a major crisis or future conflict between the People's Republic of China and the United States.

(G) Such recommendations as the task force may have for the Homeland Security Enterprise, the intelligence community, or critical infrastructure owners and operators

to improve the detection and mitigation of the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(H) A one-time plan for an awareness campaign to familiarize critical infrastructure owners and operators with security resources and support offered by Federal departments and agencies to mitigate the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China.

(4) BRIEFING.—Not later than 30 days after the date of the submission of each report under this subsection, the task force shall provide to the appropriate congressional committees a classified briefing on the findings, conclusions, and recommendations of the task force.

(5) FORM.—Each report under this subsection shall be submitted in classified form, consistent with the protection of intelligence sources and methods, but may include an unclassified executive summary.

(6) PUBLICATION.—The unclassified executive summary of each report required under this subsection shall be published on a publicly accessible website of the Department of Homeland Security.

(g) ACCESS TO INFORMATION.—

(1) IN GENERAL.—The Secretary of Homeland Security, the Director of CISA, the Attorney General, the Director of the Federal Bureau of Investigation, and the heads of appropriate Sector Risk Management Agencies, as determined by the Director of CISA, shall provide to the task force such information, documents, analysis, assessments, findings, evaluations, inspections, audits, or reviews relating to efforts to counter the cybersecurity threat posed by State-sponsored cyber actors, including Volt Typhoon, of the People's Republic of China as the task force considers necessary to carry out this section.

(2) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information, documents, analysis, assessments, findings, evaluations, inspections, audits, and reviews described in this subsection shall be received, handled, stored, and disseminated only by members of the task force consistent with all applicable statutes, regulations, and executive orders.

(3) SECURITY CLEARANCES FOR TASK FORCE MEMBERS.—No member of the task force may be provided with access to classified information under this section without the appropriate security clearances.

(h) TERMINATION.—The task force, and all the authorities of this section, shall terminate on the date that is 60 days after the final briefing required under subsection (h)(4).

(i) EXEMPTION FROM FACA.—Chapter 10 of title 5, United States Code (commonly referred to as the ''Federal Advisory Committee Act''), shall not apply to the task force.

(j) EXEMPTION FROM PAPERWORK REDUCTION ACT.—Chapter 35 of title 44, United States Code (commonly known as the ''Paperwork Reduction Act''), shall not apply to the task force.

(k) DEFINITIONS.—In this section:

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

(A) the Committee on Homeland Security, the Committee on Judiciary, and the Select Committee on Intelligence of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Judiciary, and the Select Committee on Intelligence of the Senate.

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

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(4) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(5) HOMELAND SECURITY ENTERPRISE.—The term ''Homeland Security Enterprise'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(6) INCIDENT.—The term ''incident'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(7) INFORMATION SHARING.—The term ''information sharing'' means the bidirectional sharing of timely and relevant information concerning a cybersecurity threat posed by a State-sponsored cyber actor of the People's Republic of China to United States critical infrastructure.

(8) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(9) LOCALITY.—The term ''locality'' means any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal, or other local government level.

(10) SECTOR.—The term ''sector'' means a collection of assets, systems, networks, entities, or organizations that provide or enable a common function for national security (including national defense and continuity of Government), national economic security, national public health or safety, or any combination thereof.

(11) SECTOR RISK MANAGEMENT AGENCY.—The term ''Sector Risk Management Agency'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(12) STATE.—The term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(13) SYSTEMS.—The term ''systems'' means a combination of personnel, structures, facilities, information, materials, equipment, networks, or processes, whether physical or virtual, integrated or interconnected for a specific purpose that enables an organization's services, functions, or capabilities.

(14) UNITED STATES.—The term ''United States'', when used in a geographic sense, means any State of the United States.

(15) VOLT TYPHOON.—The term ''Volt Typhoon'' means the People's Republic of China State-sponsored cyber actor described in the Cybersecurity and Infrastructure Security Agency cybersecurity advisory entitled ''PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure'', issued on February 07, 2024, or any successor advisory.

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

The Chair recognizes the gentleman from Tennessee.

□ 1500

GENERAL LEAVE

Mr. GREEN of Tennessee. Mr. 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 H.R. 9769.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Tennessee?

There was no objection.

Mr. GREEN of Tennessee. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 9769. As we have all witnessed in recent weeks, foreign malicious cyber actors are continuously attempting to infiltrate IT environments in a wide range of U.S. critical infrastructure sectors.

The DHS Strengthening Cyber Resilience Against State-Sponsored Threats Act will establish an interagency task force chaired by the Director of CISA to address the cybersecurity threats posed by PRC cyber actors, including Volt Typhoon.

I commend my colleague, the gentlewoman from Florida (Ms. LEE), for her leadership in confronting these threats. I am proud to have joined her in introducing this legislation.

Mr. Speaker, I urge my colleagues to support this legislation, and I reserve the balance of my time.

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

Mr. Speaker, our adversaries are growing bolder and more sophisticated in using cyber tools to gain access to government and critical infrastructure networks. As we speak, the Federal Government and its private-sector partners are working to understand the full scope and scale of the telecommunications hack by state-sponsored threat actors from China, known as Salt Typhoon.

The Salt Typhoon telecom hack followed warnings issued earlier this year by the Cybersecurity and Infrastructure Security Agency and its Federal partners that state-sponsored threat actors from China are ''seeking to preposition themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure.''

H.R. 9769, the Strengthening Cyber Resilience Against State-Sponsored Threats Act, formalizes interagency efforts already underway to defend against state-sponsored threat activity directed by the People's Republic of China.

Notably, it would establish an interagency task force and a reporting requirement to ensure Congress is informed of sector-specific cyber threat trends and additional resources or authorities the government needs to protect government and critical infrastructure networks, among other things.

Mr. Speaker, I urge my colleagues to support H.R. 9769, and I reserve the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I yield such time as she may consume to the gentlewoman from Florida (Ms. LEE).

Ms. LEE of Florida. Mr. Speaker, the Chinese Communist Party and other adversary nation-states and criminal networks have been exploiting our critical infrastructure and collecting information on American officials, posing a grave threat to our national security.

The malicious cyber activity by the CCP represents a calculated effort to gather intelligence on IT systems vital to U.S. national security, public safety, and economic stability.

Specifically, the CCP state-sponsored cyber actor known as Volt Typhoon has conducted a coordinated campaign to infiltrate the information technology environments of a wide range of critical infrastructure sectors of the United States, including sectors like communications, transportation, energy, and water.

H.R. 9769, the Strengthening Cyber Resilience Against State-Sponsored Threats Act, will create an interagency task force, chaired by the Cybersecurity and Infrastructure Security Agency, CISA, Director and co-chaired by the FBI Director to address the cybersecurity threat posed by CCP cyber actors.

This bill would improve our defensive and offensive capabilities in cyberspace and requires the task force to provide a classified report and briefing to Congress annually for 5 years on their findings, conclusions, and recommendations relating to malicious cyber activity. Specifically, this task force will help Congress create a mitigation strategy every year to help us prevent future cyberattacks and protect our national security.

It is time to mitigate this threat and secure our networks and infrastructure to protect all Americans. We must address the grave threats China and other foreign adversaries pose to our cybersecurity. I urge my colleagues to vote ''yes'' on H.R. 9769.

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

Mr. Speaker, I urge my colleagues to support H.R. 9769, and I yield back the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I urge my colleagues to support H.R. 9769, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Tennessee (Mr. GREEN) that the House suspend the rules and pass the bill, H.R. 9769.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

DHS CYBERSECURITY INTERNSHIP PROGRAM ACT

Mr. GREEN of Tennessee. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 9689) to amend the Homeland Security Act of 2002 to establish a DHS Cybersecurity Internship Program, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 9689

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 Cybersecurity Internship Program Act''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY INTERNSHIP PROGRAM.''.

(a) PROGRAM.—Subtitle D of title XIII of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

''SEC. 1334. CYBERSECURITY INTERNSHIP PROGRAM.

''(a) PROGRAM.—The Secretary shall carry out a cybersecurity internship program (in this section referred to as the 'Program') under which an eligible individual participates in a paid cybersecurity internship at the Department with duties aligned to such participant's respective education, skills, and experience.

''(b) ELIGIBILITY.—To be eligible to participate in the Program, an individual shall—

''(1) be a citizen of the United States;

''(2) be at least 16 years old; and

''(3) be enrolled in a secondary school, technical, trade, or vocational school, or institution of higher education, in accordance with subsection (c).

''(c) COMPOSITION.—The Secretary shall, as practicable, ensure that participants selected for the Program for each intern class include students enrolled in each of the following:

''(1) Secondary schools.

''(2) Junior or community colleges.

''(3) Undergraduate degree programs.

''(4) Postgraduate degree programs.

''(5) Technical, trade, or vocational schools.

''(d) REPORTS.—

''(1) REPORTS.—Not later than one year after the date of the enactment of this section and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the Program.

''(2) MATTERS.—Each report under paragraph (1) shall include, with respect to the most recent Program year, the following:

''(A) A description of outreach efforts by the Secretary to raise awareness of the Program among secondary schools and institutions of higher education, including among junior or community colleges, historically-Black colleges and universities, and other minority-serving institutions.

''(B) Information on specific recruiting efforts by the Secretary to increase participation in the Program.

''(C) The number of individuals participating in the Program, listed by the type of school or program in which the individual is enrolled at the time of participation, and information on the nature of each such participation, including Department components supported, and the duties of each such individual.

''(3) CONSOLIDATION.—Reports submitted under this subsection may be consolidated with the reports required under section 1333(e).

''(e) DEFINITIONS.—In this section:

''(1) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term 'historically Black college or university' has the meaning given the term 'part B institution' in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

''(2) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

''(3) JUNIOR OR COMMUNITY COLLEGE.—The term 'junior or community college' has the meaning given that term in section 312 of the Higher Education Act of 1965 (20 U.S.C. 1058).

''(4) MINORITY-SERVING INSTITUTION.—The term 'minority-serving institution' means an eligible institution of higher education described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

''(5) SECONDARY SCHOOL.—The term 'secondary school' means a school or program that provides secondary education, as determined under State law, except that the term does not include any education beyond grade 12.

''(6) TECHNICAL, TRADE, OR VOCATIONAL SCHOOL.—The term 'technical, trade, or vocational school' has the meaning given that term in section 411.167 of title 20, Code of Federal Regulations.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 1333 the following new item:

''Sec. 1334. Cybersecurity internship program.''.

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

The Chair recognizes the gentleman from Tennessee.

GENERAL LEAVE

Mr. GREEN of Tennessee. Mr. 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 H.R. 9689.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Tennessee?

There was no objection.

Mr. GREEN of Tennessee. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 9689, the DHS Cybersecurity Internship Program Act.

I thank my colleague, the gentlewoman from New York (Ms. CLARKE), for her work on this legislation.

Mr. Speaker, I urge my colleagues to support this legislation, and I reserve the balance of my time.

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

Mr. Speaker, according to testimony before the House Committee on Homeland Security earlier this year, there are approximately 2,000 cybersecurity vacancies at the Department of Homeland Security. Recent cyber intrusions like the Salt Typhoon telecom breach demonstrate the urgent need to fill those empty desks.

That is why I have introduced H.R. 9689, the DHS Cybersecurity Internship Program Act. This bill codifies DHS' cyber internship program, helping ensure DHS continues to expand its efforts to support individuals seeking to join the cyber workforce.