(H) A review of the Department's public awareness initiatives focused on the following:

(i) Educating the public on recognizing suspicious vehicle-related behavior and reporting potential threats.

(ii) Building trust and fostering collaboration between communities and law enforcement agencies.

(iii) Enhancing resilience by encouraging community-based security measures.

(I) Such other elements as the Secretary of Homeland Security considers appropriate.

(3) FORM.—The report under paragraph (1) shall be submitted in classified form, but may include an unclassified executive summary.

(4) PUBLICATION.—The unclassified executive summary of the report required under paragraph (1) shall be published on a publicly accessible website of the Department of Homeland Security.

(b) BRIEFING.—Not later than 30 days after the submission of the report under subsection (a), the Secretary of Homeland Security shall provide to the appropriate congressional committees a briefing on the findings, conclusions, and recommendations of such report.

(c) DEFINITIONS.—In this section:

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

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

(B) the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate.

(2) VEHICULAR TERRORISM.—The term ''vehicular terrorism'' means an action that utilizes automotive transportation to commit terrorism (as such term is defined in section 2(18) of the Homeland Security Act of 2002 (6 U.S.C. 101(18))).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. GARBARINO) and the gentleman from Puerto Rico (Mr. HERNÁNDEZ) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. GARBARINO. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 1608.

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

There was no objection.

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

Madam Speaker, I rise today in support of H.R. 1608, the Department of Homeland Security Vehicular Terrorism Prevention and Mitigation Act of 2025.

Following the vehicular terrorism incident in New Orleans on New Year's Day and as the U.S. prepares to host several major sporting events starting next year, it is more important than ever that the Department of Homeland Security take a leading role in addressing the threat of vehicular terrorism.

This legislation will require DHS to conduct a comprehensive assessment of emerging threats and potential countermeasures.

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

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

Madam Speaker, I rise in support of H.R. 1608, the Department of Homeland Security Vehicular Terrorism Prevention and Mitigation Act of 2025.

In the early morning on New Year's Day this year, an assailant carried out a devastating truck attack against pedestrians in New Orleans, killing 14 victims plus the perpetrator and injuring at least 57 others.

This attack is the latest in a string of attacks using vehicles to inflict significant harm.

H.R. 1608 would enhance the Department of Homeland Security's efforts to address threats posed by vehicular terrorism.

Madam Speaker, I support the bill's advancement, and I reserve the balance of my time.

Mr. GARBARINO. Madam Speaker, I yield such time as he may consume to the gentleman from Florida (Mr. GIMENEZ).

Mr. GIMENEZ. Madam Speaker, I rise today in strong support of my bill, H.R. 1608, the Department of Homeland Security Vehicular Terrorism Prevention and Mitigation Act of 2025.

On New Year's Day 2025, our Nation was shaken by a horrific ISIS-inspired attack in New Orleans that took the lives of 14 innocent people and injured dozens more.

This tragedy is a stark reminder that vehicles are increasingly being weaponized as instruments of terror. H.R. 1608 directs the Department of Homeland Security to confront the growing threat of vehicle-based attacks. It mandates a comprehensive assessment of current and emerging tactics, including the potential misuse of autonomous vehicles, rideshare platforms, and connected vehicle technologies.

Further, the bill strengthens coordination between Federal, State, and local governments and the private sector to better safeguard public gatherings, critical infrastructure, and high-density urban areas.

I thank Congressman TROY CARTER, who represents the community devastated by the New Year's Day attack, for his partnership and leadership on this effort.

This practical and bipartisan legislation is about honoring the lives we lost by doing everything possible to prevent and mitigate future attacks. With major events on the horizon, including America250, the FIFA World Cup, and the Los Angeles Olympics, we must ensure every necessary security measure is in place to protect the millions of visitors and attendees these events will bring.

Madam Speaker, I urge my colleagues to support H.R. 1608.

Mr. HERNANDEZ. Madam Speaker, I have no further speakers, and I am prepared to close.

This bill will help make life easier for all Americans by pushing DHS to advance its efforts to prevent vehicular terrorism.

Madam Speaker, I urge my colleagues to vote ''yes,'' and I yield back the balance of my time.

Mr. GARBARINO. Madam Speaker, I have no further speakers. In closing, I, again, urge my colleagues to support H.R. 1608, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. GARBARINO) that the House suspend the rules and pass the bill, H.R. 1608, 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. GARBARINO. Madam 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 motion will be postponed.

STRENGTHENING CYBER RESILIENCE AGAINST STATE-SPONSORED THREATS ACT

Mr. GARBARINO. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 2659) 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 Peoples 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. 2659

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 New York (Mr. GARBARINO) and the gentleman from Puerto Rico (Mr. HERNÁNDEZ) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. GARBARINO. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 2659.

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

There was no objection.

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

Madam Speaker, I rise today in support of H.R. 2659, the Strengthening Cyber Resilience Against State-Sponsored Threats Act.

Following the revelations of the Typhoon actors sponsored by the People's Republic of China, the committee found that the response of the previous administration was unsatisfactory. This legislation will create an interagency task force chaired by the Director of Cybersecurity and Infrastructure Security Agency to properly address the cybersecurity threat posed by the People's Republic of China's cyber actors.

Madam Speaker, I urge support, and I reserve the balance of my time.

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

Madam Speaker, I rise in support of H.R. 2659, the Strengthening Cyber Resilience Against State-Sponsored Threats Act.

This bill establishes an interagency task force to coordinate efforts to combat cyber threats from the People's Republic of China and establishes reporting requirements to ensure Congress is informed on administration efforts.

Under the Biden administration, CISA, FBI, and other Federal agencies established valuable partnerships to address the threats posed by Chinese state-backed threat actors such as Volt Typhoon and Salt Typhoon.

This bill codifies those efforts.

Unfortunately, hundreds of cybersecurity personnel have left CISA under Trump administration pressure, severely undermining the agency's ability to defend critical infrastructure from cyber threats from the PRC and other adversaries.

I hope that passing this bill will help demonstrate to the administration the need to prioritize resources and personnel on combating serious cyber threats.

Madam Speaker, I reserve the balance of my time.

□ 1650

Mr. GARBARINO. Madam Speaker, I yield such time as he may consume to the gentleman from Tennessee (Mr. OGLES).

Mr. OGLES. Madam Speaker, I rise today in support of my bill, H.R. 2659, the Strengthening Cyber Resilience Against State-Sponsored Threats Act.

Earlier this year, I introduced this legislation because the United States is facing an increasingly coordinated and persistent effort by malicious cyber actors linked to the Government of the People's Republic of China, the PRC. These groups represent one of the most serious national security challenges confronting our Nation today.

Reports from Federal agencies and private-sector partners over the past several years have shown that Chinese state-sponsored cyber actors, including Volt Typhoon, Salt Typhoon, and other PRC-affiliated groups, have been targeting the systems and services that Americans rely on every single day.

In committee, there has been testimony that 98 percent of our municipalities operate under cybersecurity poverty, meaning they don't have the resources to defend themselves. These intrusions have affected communication providers, energy operators, water systems, transportation networks, and other sectors that are fundamental to public safety and economic stability.

What has become clear is that these actors are not simply trying to collect information. In many cases, they have attempted to position themselves inside sensitive systems for long periods of time, for years, in some cases, before being discovered.

Their activity indicates preparation for the possibility of major disruption during a time of crisis, including potentially over Taiwan. This is a serious strategic concern, and it demands a serious national response.

These groups often use advanced techniques that allow them to operate quietly within everyday system activity. They rely on legitimate tools and access privileges to conceal malicious behavior. This makes detection extremely difficult and allows intrusions to remain unnoticed until long after a compromise has taken place.

While Federal agencies have taken important steps to respond, the overall effort has revealed significant challenges in the way our government organizes its cybersecurity responsibilities. Multiple agencies share roles in protecting critical infrastructure, but they operate under different missions, structures, and authorities. Through fast-moving or complex incidents, these differences can slow the exchange of information and create uncertainty about responsibility and response actions.

H.R. 2659 addresses these gaps by directing the creation of a joint interagency task force led by the Cybersecurity and Infrastructure Security Agency, CISA, in partnership with the Federal Bureau of Investigation. This task force will bring together the agencies that serve as sector risk management agencies, along with the intelligence community and other Federal partners with responsibility for critical infrastructure security.

The goal is straightforward: Federal actions must be aligned, coordinated, and based on a shared understanding of the threat environment.

The legislation also requires the task force to provide Congress with a detailed initial assessment, followed by annual reports for 5 years. These reports will offer insight into the tactics used by PRC-affiliated cyber actors, vulnerabilities across sectors, the potential impacts of disruptions during a major crisis, and any additional tools or authorities Federal agencies may need.

Classified briefings will ensure that Congress receives timely and accurate information necessary to evaluate our nationwide posture.

This bill strengthens unity and effort. It improves coordination. It increases visibility and accountability. It ensures that the United States can respond to foreign cyber aggression with preparation rather than reaction.

H.R. 2659 reflects lessons learned from real-world incidents. It elevates our national approach to cybersecurity, and it helps protect American communities from adversaries who are actively working to compromise the systems that support our way of life.

We cannot let a bureaucracy stand in the way of defending our Nation's cybersecurity. I strongly urge my colleagues to support this important legislation.

Mr. HERNÁNDEZ. Madam Speaker, I have no further speakers, and I am prepared to close when the gentleman is prepared to close. I reserve the balance of my time.

Mr. GARBARINO. Madam Speaker, I think I would be remiss if I did not mention the ranking member of the full committee and the ranking member of the subcommittee who worked so hard on getting this bill across the finish line. I am very excited that this is a very nice bipartisan effort on something that has to get done. There is a big focus that we have to have on the People's Republic of China and what they are doing when it comes to cybersecurity.

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

Ms. LEE of Florida. Madam Speaker, I rise today in support of H.R. 2659, the Strengthening Cyber Resilience Against State-Sponsored Threats Act.

I thank Congressman OGLES for his leadership on this legislation and for his commitment to enhancing the security of our Nation's critical infrastructure.

In recent years, the United States has faced an alarming surge in malicious cyber activity originating from

groups aligned with the Government of the People's Republic of China.

These actors have demonstrated a level of sophistication and planning that reflects both significant resources and a deep understanding of the essential systems that keep our country functioning.

Groups associated with the PRC, including those known as Volt Typhoon, Salt Typhoon, and others, have directed their attention toward the networks that deliver power, water, communications, transportation services, and other foundational systems relied upon by millions of Americans every day.

Their operations have shown a clear pattern. They look for ways to enter sensitive environments. They work to remain there as long as possible. They study the systems they infiltrate so that their presence blends into normal activity.

This type of long-term access is particularly concerning. When an adversary establishes persistent access to critical systems, even access that appears dormant, it creates the possibility of disruption at a future date.

The United States cannot allow foreign actors to position themselves in ways that could compromise public safety, interrupt essential services, or hinder our ability to respond in times of crisis.

The scale of targeting has also continued to expand. These cyber actors are now looking across multiple sectors at once, which means that our national response must be organized in a way that can match the breadth of the threat.

Federal responsibilities for protecting critical infrastructure are distributed across several departments, and each department has specific missions and authorities. That structure often works well during normal operations, but when confronted with a fast-moving and coordinated foreign threat, it can create gaps in communication and delay collective action.

H.R. 2659 provides a clear and practical solution to this challenge. The bill directs the creation of a joint interagency task force led by the Cybersecurity and Infrastructure Security Agency with support from the Federal Bureau of Investigation.

This task force will bring together the agencies responsible for overseeing individual sectors, the intelligence community, and other Federal partners. The purpose is to ensure that all relevant entities are sharing information, planning together, and taking action with a common understanding of the threat.

The legislation also strengthens the role of Congress by ensuring that we receive timely, comprehensive assessments of the threat landscape. These reports will help us understand sector-specific vulnerabilities, the methods used by the PRC-linked cyber actors, the potential consequences of disruption during a crisis, and the extent to which Federal agencies may need additional tools or authorities.

This ongoing visibility is vital for effective oversight and for developing policies that reflect current and emerging challenges.

H.R. 2659 is a thoughtful and necessary step toward improving the resilience of our critical infrastructure. It lays the groundwork for a more unified and prepared Federal approach. It supports the operators who manage vital systems across our country. It strengthens our national posture against a foreign adversary that has already shown its willingness to target essential American services.

I urge my colleagues to join me in supporting this important legislation.

□ 1700

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

Madam Speaker, I urge my colleagues to support H.R. 2659, and I yield back the balance of my time.

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

Madam Speaker, I urge my colleagues to support H.R. 2659. I congratulate my colleague, the gentleman from Tennessee (Mr. OGLES) on the great work he did on this bill, and I yield back the balance of my time.

The SPEAKER pro tempore (Ms. MALLIOTAKIS). The question is on the motion offered by the gentleman from New York (Mr. GARBARINO) that the House suspend the rules and pass the bill, H.R. 2659.

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. GARBARINO. Madam 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 motion will be postponed.

PROTECTING INFORMATION BY LOCAL LEADERS FOR AGENCY RESILIENCE ACT

Mr. GARBARINO. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 5078) to amend the Homeland Security Act of 2002 to reauthorize the State and local cybersecurity grant program of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5078

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 ''Protecting Information by Local Leaders for Agency Resilience Act'' or the ''PILLAR Act''.

SEC. 2. REAUTHORIZATION OF CISA STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

Section 2220A of the Homeland Security Act of 2002 (6 U.S.C. 665g) is amended—

(1) in subsection (a)—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), (6), and (7) as paragraphs (3), (4), (6), (8), (9), (10), and (11), respectively;

(B) by inserting before paragraph (3), as so redesignated, the following new paragraphs:

''(1) ARTIFICIAL INTELLIGENCE.—The term 'artificial intelligence' has the meaning given such term in section 5002(3) of the National Artificial Intelligence Initiative Act of 2020 (enacted as division E of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 9401(3))).

''(2) ARTIFICIAL INTELLIGENCE SYSTEM.—The term 'artificial intelligence system' means any data system, software, hardware, application tool, or utility that operates in whole or in part using artificial intelligence.'';

(C) by inserting after paragraph (4), as so redesignated, the following new paragraph:

''(5) FOREIGN ENTITY OF CONCERN.—The term 'foreign entity of concern' has the meaning given such term in section 10634 of the Research and Development, Competition, and Innovation Act (42 U.S.C. 19237; Public Law 117–167; popularly referred to as the 'CHIPS and Science Act').''; and

(D) by inserting after paragraph (6), as so redesignated, the following new paragraph:

''(7) MULTI-FACTOR AUTHENTICATION.—The term 'multi factor authentication' means an authentication system that requires more than one distinct type of authentication factor for successful authentication of a user, including by using a multi-factor authenticator or by combining single-factor authenticators that provide different types of factors.'';

(2) in subsection (b)(1), by striking ''information systems owned'' and inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned,'';

(3) in subsection (d)(4), by striking ''to the information systems owned'' and inserting ''to the information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned,'';

(4) in subsection (e)—

(A) in paragraph (2)—

(i) in subparagraph (A)(i), by striking ''information systems owned'' and inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned,'';

(ii) in subparagraph (B)—

(I) by amending clauses (i) through (v) to read as follows:

''(i) manage, monitor, and track applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, that are maintained, owned, or operated by, or on behalf of, the eligible entity, or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, and the information technology deployed on such information systems or operational technology systems (as the case may be), including legacy information systems, operational technology systems, and information technology that are no longer supported by the manufacturer of the systems or technology at issue;

''(ii) monitor, audit, and track network traffic and activity transiting or traveling to or from applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or operated by, or on behalf of, the eligible entity or, if the eligible