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

entity is a State, local governments within the jurisdiction of the eligible entity;

''(iii) enhance the preparation, response, and resiliency of 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 entity is a State, local governments within the jurisdiction of the eligible entity, 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 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 entity is a State, local governments within the jurisdiction of the eligible entity;

''(v) ensure that the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, adopt and use best practices and methodologies to enhance cybersecurity, particularly identity and access management solutions such as multi-factor authentication, which may include—

''(I) the practices set forth in a cybersecurity framework developed by the National Institute of Standards and Technology or the Agency;

''(II) cyber chain supply chain risk management best practices identified by the National Institute of Standards and Technology or the Agency;

''(III) knowledge bases of adversary tools and tactics;

''(IV) technologies such as artificial intelligence; and

''(V) improving cyber incident response capabilities through adoption of automated cybersecurity practices;'';

(II) in clause (x), by inserting ''or operational technology systems, including either or both of such systems using artificial intelligence,'' after ''information systems'';

(III) in clause (xi)(I), by inserting '', including through Department of Homeland Security State, Local, and Regional Fusion Center Initiative under section 210(A)'' before the semicolon;

(IV) in clause (xii), by inserting '', including for bolstering the resilience of outdated or vulnerable information systems or operational technology systems, including either or both of such systems using artificial intelligence'' before the semicolon;

(V) by amending clause (xiii) to read as follows:

''(xiii) implement an information technology or operational technology, including either or both of such systems using artificial intelligence, modernization cybersecurity review process that ensures alignment between information technology, operational technology, and artificial intelligence cybersecurity objectives;'';

(VI) in clause (xiv)(II)—

(aa) in item (aa), by striking ''and'' after the semicolon;

(bb) in item (bb), by inserting ''and'' after the semicolon; and

(cc) by adding at the end the following new item:

''(cc) academic and nonprofit entities, including cybersecurity clinics and other nonprofit technical assistance programs;''; and

(VII) by amending clause (xv) to read as follows:

''(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas and other local governments with small populations within the jurisdiction of the eligible entity, including by direct outreach to such rural areas and local governments with small populations; and''; and

(iii) in subparagraph (F)—

(I) in clause (i), by striking ''and'' after the semicolon;

(II) by amending clause (ii) to read as follows:

''(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems or 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 entity is a State, local governments within the jurisdiction of the eligible entity; and''; and

(III) by adding at the end the following new clause:

''(iii) assuming the cost or partial cost of cybersecurity investments made as a result of the plan.''; and

(B) in paragraph (3)(A), by striking ''the Multi-State Information Sharing and Analysis Center'' and inserting ''Information Sharing and Analysis Organizations'';

(5) in subsection (g)—

(A) in paragraph (2)(A)(ii), by inserting ''including, as appropriate, representatives of rural, suburban, and high-population jurisdictions (including such jurisdictions with low or otherwise limited operating budgets)'' before the semicolon; and

(B) by amending paragraph (5) to read as follows:

''(5) RULE OF CONSTRUCTION REGARDING CONTROL OF CERTAIN INFORMATION SYSTEMS OR OPERATIONAL TECHNOLOGY SYSTEMS OF ELIGIBLE ENTITIES.—Nothing in this subsection may be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this subsection to make decisions relating to information systems or 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.'';

(6) in subsection (i)—

(A) in paragraph (1)(B), by striking ''2-year period'' and inserting ''3-year period'';

(B) in paragraph (3)—

(i) in the matter preceding subparagraph (A), by striking ''2023'' and inserting ''2027''; and

(ii) in subparagraph (B), by striking ''2023'' and inserting ''2027''; and

(C) in paragraph (4)—

(i) in the matter preceding subparagraph (A), by striking ''shall'' and inserting ''may''; and

(ii) in subparagraph (A), 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,'';

(7) in subsection (j)(1)—

(A) in subparagraph (D), by striking ''or'' after the semicolon;

(B) in subparagraph (E)—

(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,''; and

(ii) by striking the period and inserting a semicolon; and

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

''(F) to purchase software or hardware, or products or services of such software or hardware, as the case may be, that do not align with guidance relevant to such software or hardware, or products or services, as the case may be, provided by the Agency, including Secure by Design or successor guidance; or

''(G) to purchase software or hardware, or products or services of such software or hardware, as the case may be, that are designed, developed, operated, maintained, manufactured, or sold by a foreign entity of concern and do not align with guidance provided by the Agency.'';

(8) in subsection (l), in the matter preceding paragraph (1), by striking ''2022'' and inserting ''2026'';

(9) in subsection (m), by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—The Federal share of activities carried out using funds made available pursuant to the award of a grant under this section may not exceed—

''(A) in the case of a grant to an eligible entity, 60 percent for each fiscal year through fiscal year 2033; and

''(B) in the case of a grant to a multi-entity group, 70 percent for each fiscal year through fiscal year 2033.

Notwithstanding subparagraphs (A) and (B), the Federal share of the cost for an eligible entity or multi-entity group shall be 65 percent for an entity and 75 percent for a multi-group entity for each fiscal year beginning with fiscal year 2028 through fiscal year 2033 if such entity or multi-entity group entity, as the case may be, implements or enables, by not later than October 1, 2027, multi-factor authentication and identity and access management tools that support multi-factor authentication with respect to critical infrastructure, including the information systems and operational technology systems, including either or both of such systems using artificial intelligence, of such critical infrastructure, that is within the jurisdiction of such entity or multi-entity group is responsible.'';

(10) in subsection (n)—

(A) in paragraph (2)—

(i) in subparagraph (A)—

(I) in the matter preceding clause (i), by striking ''a grant'' and inserting ''a grant on or after January 1, 2026, or changes the allocation of funding as permissible within the allowances''; and

(II) by amending clauses (ii) and (iii) to read as follows:

''(ii) with the consent of the local governments, items, in-kind services, capabilities, or activities, or a combination of funding and other services, having a value of not less than 80 percent of the amount of the grant; or

''(iii) with the consent of the local governments, grant funds combined with other items, in-kind services, capabilities, or activities, or a combination of funding and other services, having the total value of not less than 80 percent of the amount of the grant.''; and

(ii) in subparagraph (B), by amending clauses (ii) and (iii) to read as follows:

''(ii) items, in kind services, capabilities, or activities, or a combination of funding and other services, having a value of not less than 25 percent of the amount of the grant awarded to the eligible entity; or

''(iii) grant funds combined with other items, in kind services, capabilities, or activities, or a combination of funding and other services, having the total value of not less than 25 percent of the grant awarded to the eligible entity.''; and

(B) by amending paragraph (5) to read as follows:

''(5) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local government required under paragraph (2) within

60 days of the anticipated grant disbursement date, such local government may petition the Secretary to request the Secretary to provide funds directly to such local government.'';

(11) in subsection (o), in the matter preceding paragraph (1), by inserting ''and representatives from rural areas and other local governments with small populations'' after ''governments'';

(12) by redesignating subsections (p) through (s) as subsections (q) through (t), respectively;

(13) by inserting after subsection (o) the following new subsection:

''(p) OUTREACH TO LOCAL GOVERNMENTS.—The Secretary, acting through the Director, shall implement an outreach plan to inform local governments, including those in rural areas or with small populations, about no-cost cybersecurity service offerings available from the Agency.'';

(14) in subsection (r), as so redesignated—

(A) in paragraph (1)(A)—

(i) in clause (i), by striking ''and'' after the semicolon;

(ii) in clause (ii)—

(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,''; and

(II) by striking the period and inserting ''; and''; and

(iii) by adding at the end the following new clause:

''(iii) assuming the costs associated with continuing the programs specified in the Cybersecurity Plan by including such programs in State and local government budgets upon full expenditure of grant funds by the eligible entity.'';

(B) in paragraph (2)(E)(ii), 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''; and

(C) by amending paragraph (6) to read as follows:

''(6) GAO REVIEW.—Not later than three years after the date of the enactment of this paragraph and every three years thereafter until the termination of the State and Local Cybersecurity Grant Program, the Comptroller General of the United States shall conduct a review of the Program, including relating to the following:

''(A) The grant selection process of the Secretary.

''(B) A sample of grants awarded under this section.

''(C) A review of artificial intelligence adoption across the sample of grants reviewed.'';

(15) in subsection (s), as so redesignated, by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—The activities under this section are subject to the availability of appropriations.''; and

(16) in subsection (t), as so redesignated, in paragraph (1), by striking ''2025'' and inserting ''2033''.

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 may have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 5078.

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. 5078, the Protecting Information by Local Leaders for Agency Resilience Act, also known as the PILLAR Act.

Madam Speaker, I first thank Congressman OGLES for his leadership in bringing forward this bipartisan bill.

Cybersecurity is often discussed in the context of national systems, but the truth is that many of the most disruptive incidents occur in our own communities.

In recent years, local governments across the country have experienced attacks that shut down city services, delayed school operations, locked police and court records, and forced jurisdictions of all sizes to spend significant funds on recovery. These events may not always make national headlines, but they have real consequences for families, businesses, and public safety.

Some of these attacks come from criminal ransomware groups, while others originate from foreign adversaries that seek to test the resilience of American communities. The Committee on Homeland Security has monitored these trends closely.

A recent cyber-threat snapshot shows that the majority of States have experienced significant cyber incidents at the local level this year, and many of those incidents targeted smaller jurisdictions that have limited staff, outdated systems, and fewer resources to defend themselves.

Finally, this bill is the product of bipartisan work. It passed through the Committee on Homeland Security with support from Members across the political spectrum. I especially thank Representatives SWALWELL and EVANS for their work alongside myself and Congressman OGLES to advance this important legislation. That cooperation reflects a shared recognition that cybersecurity cannot be approached through a partisan lens.

By passing the PILLAR Act, the House can reaffirm its commitment to our State, local, Tribal, and territorial partners. When our communities are more secure, our entire Nation is more secure.

I thank Congressman OGLES, again, for his leadership in bringing forward this bipartisan bill.

Madam Speaker, I urge my colleagues to support H.R. 5078, 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. 5078, which reauthorizes the State and Local Cybersecurity Grant Program until 2033.

First established 4 years ago in the bipartisan infrastructure law based on legislation authored by Representative YVETTE CLARKE, the State and Local Cybersecurity Grant Program has provided $1 billion in funding for State, local, Tribal, and territorial governments so that they can strengthen their cyber defenses.

Earlier this year, the Cybersecurity Subcommittee held a hearing to evaluate the program and receive testimony from the National League of Cities, the National Association of State Chief Information Officers, and one of the Nation's top cybersecurity firms. Their assessment was clear: The State and Local Cybersecurity Grant Program has worked.

From Connecticut to Kentucky to Utah, the State and Local Cybersecurity Grant Program has forged partnerships that have helped detect and thwart attacks, built resilience, and stretched dollars further.

From municipal services to our school systems, the services that our constituents rely on every day are more secure today than they were 4 years ago, but our work is not done. Despite the impressive progress that State and local governments have made to improve their cybersecurity posture, many jurisdictions across the country, particularly rural areas, remain unacceptably vulnerable to cyberattacks.

Every day, State and local governments must defend against cyber intrusions from transnational criminal gangs and nation-state adversaries. The Federal Government has an obligation to leverage its resources, expertise, and intelligence to defend our State and local governments from these sophisticated threats.

There are no other circumstances under which we would expect a State or local government to defend itself from an attack from a state actor, particularly from China, Russia, or Iran. With this essential program's authorization set to expire on January 30, enacting a long-term reauthorization will help provide stability to the program and, importantly, build a case for appropriating more funding for it.

At a time when the Trump administration has been cutting vital cybersecurity resources for State and local governments, such as the Multi-State Information Sharing and Analysis Center, it is more important than ever that Congress step up to provide more funding for State and local cybersecurity.

Madam Speaker, I reserve the balance of my time.

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

Mr. OGLES. Madam Speaker, I thank the gentleman for yielding.

Madam Speaker, I rise today in support of my bill, H.R. 5078, the Protecting Information by Local Leaders for Agency Resilience Act, known as the PILLAR Act.

This legislation is about strengthening the first line of defense in our Nation's cybersecurity. While we often focus on Federal networks and high-profile national systems, the reality is that many of the services Americans depend on every single day are run by State and local governments.

When a resident pays a utility bill online, when a police department dispatches an officer, or when a hospital connects to a county network, all of those activities rely on State and local systems that are now squarely in the sights of foreign adversaries and criminal groups.

As a former county executive in Tennessee, I saw firsthand how limited budgets, aging systems, and staffing constraints can leave local governments struggling to keep up with modern cyber threats.

Many smaller jurisdictions only operate with a handful of IT staff and, in some cases, with none at all. Yet, they are expected to defend against the same nation-state actors that target major corporations and Federal agencies. That is not a fair fight, and it is not a sustainable model for national security.

The State and Local Cybersecurity Grant Program at the Department of Homeland Security was created to help close that gap by providing targeted assistance to those States, territories, and local governments so that they can assess the risk, modernize outdated systems, and build real cyber resilience.

The PILLAR Act reauthorizes and strengthens this program so that it reflects the threat environment we face today and the technological landscape that State and local partners are actually operating in.

This bill makes several important updates. It ensures that the program covers not only traditional information technology systems but also operational technology and systems that incorporate artificial intelligence. That means that we are recognizing the reality that cyber risk now extends to everything from industrial control systems at water treatment plants to connected devices at public safety networks to AI-enabled tools used by local agencies.

The bill encourages the adoption of basic but powerful best practices, such as multifactor authentication and stronger identity and access management tools across State and local networks.

It promotes continuous vulnerability assessment and monitoring so that jurisdictions can detect and mitigate threats before those threats turn into major incidents. It also emphasizes the importance of good cyber hygiene, modern configuration management, and alignment with frameworks developed by CISA and the National Institute of Standards and Technology.

Importantly, the PILLAR Act recognizes that not all communities start from the same place. It directs outreach and support to rural areas and jurisdictions with small populations, which are often the least resourced but still operate critical services.

It encourages partnerships with academic and nonprofit organizations, including cybersecurity clinics and other technical assistance providers that can help these communities develop and implement their cyber plans. This bill also guards against the use of Federal grant dollars on technology that introduces additional risk.

□ 1710

It prohibits the use of funds to purchase software or hardware from foreign entities of concern when those products do not align with CISA guidance, and it directs grantees to follow secure-by-design recommendations so that public money is not spent on tools that undermine security.

We also provide more predictability around cost share requirements so that States and local governments can plan over the long term.

The legislation maintains a strong Federal commitment while encouraging jurisdictions to invest in sustaining the improvements they make.

For those that implement multifactor authentication and related protections by a certain date, the bill provides additional flexibility in the Federal cost share to reward that proactive work.

This is a bipartisan bill. I am proud to have worked closely with Chairman GARBARINO and Representatives SWALWELL and EVANS on this critical legislation, and appreciate the support it has received from Members on both sides of the aisle.

We share the same goal, which is to help our communities defend themselves against increasingly sophisticated cyber threats and to ensure continuity of essential services for the American people.

Supporting the PILLAR Act is about more than technology. It is about public trust. When a local government falls victim to ransomware and emergency services are delayed, when a school district loses student records, or when basic services are interrupted, citizens lose confidence in those institutions.

This bill helps prevent those outcomes by equipping State and local leaders with the resources and tools they need to prepare.

Madam Speaker, I urge my colleagues to support H.R. 5078 and to stand with the State, local, Tribal, and territorial partners who are on the front lines of our cyber defense every day.

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

Madam Speaker, I urge my colleagues to support H.R. 5078, and I yield back the balance of my time.

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

Madam Speaker, I, again, urge my colleagues to support H.R. 5078, 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. 5078, as amended.

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

A motion to reconsider was laid on the table.

BOTTLES AND BREASTFEEDING EQUIPMENT SCREENING ENHANCEMENT ACT

Mr. GARBARINO. Madam Speaker, I move to suspend the rules and pass the bill (S. 260) to amend the Bottles and Breastfeeding Equipment Screening Act to require hygienic handling of breast milk and baby formula by security screening personnel of the Transportation Security Administration and personnel of private security companies providing security screening, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 260

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 ''Bottles and Breastfeeding Equipment Screening Enhancement Act''.

SEC. 2. HYGIENIC HANDLING OF BREAST MILK AND BABY FORMULA DURING AVIATION SECURITY SCREENING.

The Bottles and Breastfeeding Equipment Screening Act (Public Law 114–293) is amended by adding at the end the following new sections:

''SEC. 3. HYGIENIC HANDLING OF BREAST MILK AND BABY FORMULA DURING AVIATION SECURITY SCREENING.

''Not later than 90 days after the date of the enactment of this section and every five years thereafter, if appropriate, the Administrator of the Transportation Security Administration shall issue or update, as the case may be, guidance to minimize the risk for contamination of any breast milk, baby formula, purified deionized water for infants, and juice (as well as ice packs, freezer packs, frozen gel packs and other accessories required to cool breast milk, baby formula, and juice) that is subject to re-screening or otherwise subject to additional screening. Such guidance shall—

''(1) be developed in consultation with nationally recognized maternal health organizations;

''(2) ensure adherence to hygienic standards, as established by the Administrator, in consultation with nationally recognized maternal health organizations;

''(3) ensure that, when any such re-screening or additional screening requires additional testing, such testing so adheres to such standards, to so minimize such risk; and

''(4) apply to security screening personnel of the Administration and personnel of private security companies providing security screening pursuant to section 44920 of title 49, United States Code.

''SEC. 4. INSPECTOR GENERAL AUDIT.

''Not later than one year after the date of the enactment of this section, the Inspector General of the Department of Homeland Security shall submit to the Committee on