The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. MALINOWSKI) that the House suspend the rules and pass the bill, H.R. 6824, 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. ROY. Mr. Speaker, on that I demand the yeas and nays.

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

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

STATE AND LOCAL GOVERNMENT CYBERSECURITY ACT OF 2021

Mr. MALINOWSKI. Mr. Speaker, I move to suspend the rules and pass the bill (S. 2520) to amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal, and territorial governments, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 2520

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''State and Local Government Cybersecurity Act of 2021''.

SEC. 2. AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002.

Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2201 (6 U.S.C. 651), by adding at the end the following:

''(7) SLTT ENTITY.—The term 'SLTT entity' means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof.''; and

(2) in section 2209 (6 U.S.C. 659)—

(A) in subsection (c)(6), by inserting ''operational and'' before ''timely'';

(B) in subsection (d)(1)(E), by inserting '', including an entity that collaborates with election officials,'' after ''governments''; and

(C) by adding at the end the following:

''(p) COORDINATION ON CYBERSECURITY FOR SLTT ENTITIES.—

''(1) COORDINATION.—The Center shall, upon request and to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

''(A) conduct exercises with SLTT entities;

''(B) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—

''(i) cyber threat indicators;

''(ii) defensive measures;

''(iii) cybersecurity risks;

''(iv) vulnerabilities; and

''(v) incident response and management;

''(C) in order to increase situational awareness and help prevent incidents, assist SLTT entities in sharing, in real time, with the Federal Government as well as among SLTT entities, actionable—

''(i) cyber threat indicators;

''(ii) defensive measures;

''(iii) information about cybersecurity risks; and

''(iv) information about incidents;

''(D) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;

''(E) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—

''(i) information about tools;

''(ii) information about products;

''(iii) resources;

''(iv) policies;

''(v) guidelines;

''(vi) controls; and

''(vii) other cybersecurity standards and best practices and procedures related to information security, including, as appropriate, information produced by other Federal agencies;

''(F) work with senior SLTT entity officials, including chief information officers and senior election officials and through national associations, to coordinate the effective implementation by SLTT entities of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure the information systems, including election systems, of SLTT entities;

''(G) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;

''(H) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and

''(I) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

''(q) REPORT.—Not later than 1 year after the date of enactment of this subsection, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the services and capabilities that the Agency directly and indirectly provides to SLTT entities.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. MALINOWSKI) and the gentleman from Kansas (Mr. LATURNER) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey.

GENERAL LEAVE

Mr. MALINOWSKI. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

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

There was no objection.

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

Mr. Speaker, in recent months the world has watched in horror as Russia launched its unprovoked and illegal invasion of Ukraine. Russia's actions have, once again, reminded us of the potential for cyberattacks on critical infrastructure here in the United States.

With State and local governments operating large amounts of critical infrastructure, including essential public services like schools, emergency response agencies, and water utilities, it is essential that State and local governments have strong cybersecurity practices.

In March, in response to the current threat landscape, President Biden sent a letter to the Nation's Governors urging them to take actions to enhance their cyber defenses. The Federal Government must continue to expand our partnerships with States as they carry out this important national security work.

Congress has already taken some critical steps in this effort this Congress, thanks to the leadership of my colleagues on the Homeland Security Committee. Last year, the House passed Congresswoman YVETTE CLARKE's State and Local Cybersecurity Improvement Act which created a new grant program to assist State, local, Tribal, and territorial Governments with strengthening their cybersecurity. This legislation was signed by President Biden in the fall as part of the bipartisan infrastructure law and will provide $1 billion in much-needed help over the next 4 years.

Additionally, last year, Congress passed the K–12 Cybersecurity Act introduced by Senator PETERS and Congressman LANGEVIN. That bill directs the Cybersecurity and Infrastructure Security Agency to study the cyber risks posed to K–12 educational institutions and provide them with additional resources to better defend themselves.

Right now, I am proud to be working on a bipartisan basis with Senators Peters and Cornyn, and my Homeland Security Committee colleague Representative GARBARINO, on the Satellite Cybersecurity Act, urgently needed legislation to better protect critical infrastructure used at the municipal, State, and Federal level that relies on commercial satellite data to work properly.

Passing S. 2520 will build on these efforts by further strengthening the relationship between DHS and State and local Governments as they work to defend our country against cyberattacks. More specifically, it would permit DHS to provide State and local Governments with access to cybersecurity resources and encourage collaboration in using these resources, including joint cybersecurity exercises.

□ 1430

Additionally, the bill will strengthen the relationship between DHS and the Multi State Information Sharing and Analysis Center to help State and local governments receive the most updated information regarding potential threats and gain access to greater technical assistance.

I thank Senators PETERS and PORTMAN for their leadership in introducing this bill, I urge my colleagues to support the legislation, and I reserve the balance of my time.

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

Mr. Speaker, I rise today in support of S. 2520, the State and Local Government Cybersecurity Act of 2021.

Today, State and local governments are not in the position to defend their networks against cyberattacks from sophisticated foreign adversaries or cybercriminals. State and local governments are rich targets for cyber adversaries, and the frequency of attacks is only accelerating as budgets are increasingly constrained.

The Federal Government needs to redouble their efforts to support State, local, Tribal, and territorial government entities to bolster their cybersecurity posture.

To help remedy this, this bill amends the Homeland Security Act of 2002 to provide for engagements with SLTT entities to increase Federal support and information sharing.

Additionally, the bill expands DHS' responsibilities concerning grants and cooperative agreements. The bill also provides DHS the ability to coordinate with SLTT entities to conduct exercises, provide technical and operational cybersecurity training, as well as promote cybersecurity education and awareness.

S. 2520 will help shore up SLTT vulnerabilities against malicious cyberattackers and will go a long way to strengthen our more localized entities that are closer to the everyday American.

I urge Members to join me in supporting S. 2520, and I yield back the balance of my time.

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

Mr. Speaker, we rely on State and local governments for some of our most basic and necessary public services. We have seen many communities across the country experience disruptions in those vital services due to ransomware attacks originating from Russia.

In this current threat environment, with a heightened risk of even more dangerous cyberattacks, S. 2520 would enhance DHS's collaboration with State and local governments in addressing this pressing national security threat.

By passing this bill and sending it to the President, we will continue our ongoing efforts to expand critical Federal cybersecurity assistance to State and local governments.

Mr. Speaker, I urge my colleagues to support S. 2520, 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 Jersey (Mr. MALINOWSKI) that the House suspend the rules and pass the bill, S. 2520.

The question was taken.

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

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

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

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

BOMBING PREVENTION ACT OF 2022

Mr. MALINOWSKI. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6873) to amend the Homeland Security Act of 2002 to establish the Office for Bombing Prevention to address terrorist explosive threats, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6873

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 ''Bombing Prevention Act of 2022''.

SEC. 2. OFFICE FOR BOMBING PREVENTION.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new subtitle:

''Subtitle D—Bombing Prevention

''SEC. 2241. OFFICE FOR BOMBING PREVENTION.

''(a) ESTABLISHMENT.—There is established within the Department an Office for Bombing Prevention (in this section referred to as the 'Office').

''(b) ACTIVITIES.—The Office shall have the primary responsibility within the Department for enhancing the ability and coordinating the efforts of the United States to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States, including by carrying out the following:

''(1) Advising the Secretary on matters related to terrorist explosive threats and attacks in the United States.

''(2) Coordinating the efforts of the Department to counter terrorist explosive threats and attacks in the United States, including by carrying out the following:

''(A) Developing, in coordination with the Under Secretary for Strategy, Policy, and Plans, the Department's strategy against terrorist explosives threats and attacks, including efforts to support the security and preparedness of critical infrastructure and the public sector and private sector.

''(B) Leading the prioritization of the Department's efforts against terrorist explosive threats and attacks, including preparedness and operational requirements.

''(C) Ensuring, in coordination with the Under Secretary for Science and Technology and the Administrator of the Federal Emergency Management Agency, the identification, evaluation, and availability of effective technology applications through field pilot testing and acquisition of such technology applications by the public sector to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States.

''(D) Providing advice and recommendations to the Administrator of the Federal Emergency Management Agency regarding the effective use of grants authorized under section 2002.

''(E) In coordination with the Assistant Secretary for Countering Weapons of Mass Destruction, aligning Department efforts related to terrorist explosive threats and attacks in the United States and weapons of mass destruction.

''(3) Engaging other Federal departments and agencies, including Sector Risk Management Agencies, regarding terrorist explosive threats and attacks in the United States.

''(4) Facilitating information sharing and decision support of the public and private sector involved in deterrence, detection, prevention, protection against, mitigation of, and response to terrorist explosive threats and attacks in the United States. Such sharing and support may include the following:

''(A) Operating and maintaining a secure information sharing system that allows the sharing of critical information and data relating to terrorist explosive attack tactics, techniques, procedures, and security capabilities, including information and data described in paragraph (6) and section 2242.

''(B) Working with international partners, in coordination with the Office for International Affairs of the Department, to develop and share effective practices to deter, prevent, detect, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States.

''(5) Promoting security awareness among the public and private sector and the general public regarding the risks posed by the misuse of explosive precursor chemicals and other bomb-making materials.

''(6) Providing training, guidance, assessments, and planning assistance to the public and private sector, as appropriate, to help counter the risk of terrorist explosive threats and attacks in the United States.

''(7) Conducting analysis and planning for the capabilities and requirements necessary for the public and private sector, as appropriate, to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States by carrying out the following:

''(A) Maintaining a database on capabilities and requirements, including capabilities and requirements of public safety bomb squads, explosive detection canine teams, special tactics teams, public safety dive teams, and recipients of services described in section 2242.

''(B) Applying the analysis derived from the database described in subparagraph (A) with respect to the following:

''(i) Evaluating progress toward closing identified gaps relating to national strategic goals and standards related to deterring, detecting, preventing, protecting against, mitigating, and responding to terrorist explosive threats and attacks in the United States.

''(ii) Informing decisions relating to homeland security policy, assistance, training, research, development efforts, testing and evaluation, and related requirements regarding deterring, detecting, preventing, protecting against, mitigating, and responding to terrorist explosive threats and attacks in the United States.

''(8) Promoting secure information sharing of sensitive material and promoting security awareness, including by carrying out the following:

''(A) Operating and maintaining a secure information sharing system that allows the sharing among and between the public and private sector of critical information relating to explosive attack tactics, techniques, and procedures.

''(B) Educating the public and private sectors about explosive precursor chemicals.

''(C) Working with international partners, in coordination with the Office for International Affairs of the Department, to develop and share effective practices to deter, detect, prevent, protect against, mitigate, and respond to terrorist explosive threats and attacks in the United States.

''(D) Executing national public awareness and vigilance campaigns relating to terrorist explosive threats and attacks in the United States, preventing explosive attacks, and activities and measures underway to safeguard the United States.

''(E) Working with relevant stakeholder organizations.

''(9) Providing any other assistance the Secretary determines necessary.