organization, the Howard Area Lion's Club, so I know firsthand the good that this club does around the world.

Just a few years ago, during a Lion's Club reception at the Capitol Visitor Center, I spoke with a Lion named Jimmy Ross. Jimmy is a past president of Lions Club International, and he organized the Capitol Hill visit that year. He shared an idea to create a congressional caucus to highlight the work and the policies of nonprofit service organizations like Lions, Rotary, Kiwanis, Optimist, and others, and I loved the idea.

Together with Congressman JIMMY PANETTA of California, who is a Rotarian, we founded the Congressional Service Organization Caucus in 2019. Tomorrow, the Congressional Service Organization Caucus will host its first briefing. Speakers from Lions, Rotary, Kiwanis, and Optimist clubs will share how their members strive to make the world a better place one community at a time.

Mr. Speaker, I urge my colleagues to join the Congressional Service Organization Caucus to ensure that service to others remains a vital part of American life for generations to come.

CRISIS AT THE SOUTHERN BORDER

(Mr. ROY asked and was given permission to address the House for 1 minute.)

Mr. ROY. Mr. Speaker, I wasn't going to use this 1-minute time, but I just got a text from some contacts down on the border in south Texas from Eagle Pass with drone footage of yet another enormous group that is crossing illegally onto private property around Eagle Pass. A Texas soldier tells us that there have been 2,000-plus crossings in this specific spot in the last 8 days, yet the Secretary of Homeland Security testified in the House Judiciary Committee that ''he and this administration have operational control of the border.''

But this is factually incorrect.

My colleagues on the other side of the aisle do not seem interested in having a debate or a discussion here on the floor of the people's House about a crisis facing the State of Texas and the entire country. Over 107,000 Americans died last year from drug poisonings and drug overdoses, yet I get crickets from my colleagues on the other side of the aisle.

Mr. Speaker, do you want to know what is happening in south Texas?

Hispanics in south Texas are flocking away from a party that doesn't care if they suffer or if migrants suffer while dead bodies rack up in the Rio Grande and the ranches of south Texas. They have had enough, I have had enough, and the people of Texas have had enough.

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 the yeas and nays are ordered.

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

PRESIDENT'S CUP CYBERSECURITY COMPETITION ACT

Mr. MALINOWSKI. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6824) to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to hold an annual cybersecurity competition relating to offensive and defensive cybersecurity disciplines, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6824

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 ''President's Cup Cybersecurity Competition Act''.

SEC. 2. PRESIDENT'S CUP CYBERSECURITY COMPETITION.

(a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the ''Director'') of the Department of Homeland Security is authorized to hold an annual cybersecurity competition to be known as the ''Department of Homeland Security Cybersecurity and Infrastructure Security Agency's President's Cup Cybersecurity Competition'' (in this section referred to as the ''competition'') for the purpose of identifying, challenging, and competitively awarding prizes, including cash prizes, to the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.

(b) COMPETITION DESIGN.—

(1) IN GENERAL.—Notwithstanding section 1342 of title 31, United States Code, the Director, in carrying out the competition, may consult with, and consider advice from, any person who has experience or expertise in the development, design, or execution of cybersecurity competitions.

(2) LIMITATION.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to consultations pursuant to this section.

(3) PROHIBITION.—A person with whom the Director consults under paragraph (1) may not—

(A) receive pay by reason of being so consulted; or

(B) be considered an employee of the Federal Government by reason of so consulting.

(c) ELIGIBILITY.—To be eligible to participate in the competition, an individual shall be a Federal civilian employee or member of the uniformed services (as such term is defined in section 2101(3) of title 5, United States Code) and shall comply with any rules promulgated by the Director regarding the competition.

(d) COMPETITION ADMINISTRATION.—The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or nonprofit entity or State or local government agency to administer the competition.

(e) COMPETITION PARAMETERS.—Each competition shall incorporate the following elements:

(1) Cybersecurity skills outlined in the National Initiative for Cybersecurity Education Framework, or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.

(4) Any other elements related to paragraphs (1), (2), or (3) as determined necessary by the Director.

(f) USE OF FUNDS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, the Director may use amounts made available to the Director for the competition for the following:

(A) Advertising, marketing, and promoting the competition.

(B) Meals for participants and organizers of the competition if attendance at the meal during the competition is necessary to maintain the integrity of the competition.

(C) Promotional items, including merchandise and apparel.

(D) Monetary and nonmonetary awards for competition participants, including members of the uniformed services.

(E) Necessary expenses for the honorary recognition of competition participants, including members of the uniformed services.

(F) Any other appropriate activity necessary to carry out the competition, as determined by the Director.

(2) APPLICATION.—This subsection shall apply to amounts appropriated on or after the date of the enactment of this Act.

(g) PRIZE LIMITATION.—The Director may make one or more awards per competition, except that the amount or value of each shall not exceed $10,000. The Secretary of Homeland Security may make one or more awards per competition, except the amount or the value of each shall not to exceed $25,000. A monetary award under this section shall be in addition to the regular pay of the recipient.

(h) REPORTING REQUIREMENTS.—The Director shall annually provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following:

(1) A description of available funds under subsection (f) for each competition conducted in the preceding year.

(2) A description of expenditures authorized in subsection (g) for each competition.

(3) Information relating to the participation of each competition.

(4) Information relating to lessons learned from each competition and how such lessons may be applied to improve cybersecurity operations and recruitment of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

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, before I begin debate on today's legislation, I will take a moment to acknowledge the tragic, bloody events of this weekend in Milwaukee, Buffalo, and Orange County, California. The loss of life and extent of injury to innocent people, as we all know, are staggering.

These incidents are all under investigation but, from a homeland security perspective, I will zero in, in particular, on the events in New York where we have, I think, a fairly good picture of what motivated a man to gun down innocent people, an event that has happened too many times in recent history in our country.

This young man clearly was motivated by an idea, a hateful idea and a racist idea, and one that is sadly familiar to us. It is the same idea that motivated another man to gun down African Americans in Charleston, South Carolina. It is the same idea that motivated yet another man to gun down Hispanic Americans in El Paso, Texas. It is the same idea that motivated another man to gun down Jewish Americans in Pittsburgh, Pennsylvania.

It is an idea that spreads on the internet. But it doesn't just spread organically. Social media companies write algorithms deliberately designed to connect people who are susceptible to this hateful idea to others who may be propagating it. It is an idea that sadly is sometimes amplified and legitimized by political leaders and media personalities in our country.

We have a domestic terrorism problem in America. We all understand that on the Homeland Security Committee. If this problem was coming from outside the United States, it would be easy for us to come together to deal with it.

Imagine if after the September 11 attacks there were cable news hosts who night after night propagated ideas straight from al-Qaida's propaganda materials. We wouldn't tolerate it. Nobody would for one moment think that was acceptable in the United States of America. But because it is a domestic problem rooted in our own society, it is harder. We have to find a way to come together, nonetheless.

I think there are two kinds of leaders in America today, not Democrat, Republican, liberal, or conservative. There are leaders who, when they see a fire burning, they reach for a bucket of water to put it out. And there are leaders who, when they see a fire burning, reach for a can of gasoline to make that fire burn even more. We desperately need leaders in this country, of both political parties, who will try to calm things down and who will tamp down these horrible, hateful ideas, whether they are coming from the left or the right, wherever they are coming from, because these ideas are leading to people being gunned down in our country. It is unacceptable, and it has to stop.

Mr. Speaker, let's turn to the legislation before us today.

Mr. Speaker, as a nation, we are fortunate to have so many dedicated public servants who work for our Federal Government and help keep us safe. Unfortunately, they frequently go without the recognition they deserve for their hard work. The President's Cup Cybersecurity Competition Act authorizes an innovative prize competition where cyber talent within the ranks of Federal departments and agencies is honored.

Today, it is critical to our homeland and national security that the Federal Government attract, develop, and retain dedicated and talented employees to carry out cybersecurity and cyber defense activities. It is not lost on me that, by choosing to work for the government rather than the private sector, these in-demand professionals often forgo more lucrative career opportunities.

H.R. 6824 would authorize the cyber competition that CISA hosts and ensure that financial awards can be provided to the winning individuals and teams in recognition of their achievement. In the short period of time that the President's Cup has been around, it has become a much-sought-after prize among talented Federal cyber practitioners, many of whom are civilians or active military. By permanently authorizing this competition, Congress can ensure that it remains a vital part of our strategy to identify, retain, and reward the best cybersecurity talent in the Federal Government.

Mr. Speaker, I applaud Representative LURIA for her leadership in authoring this legislation.

Mr. Speaker, I urge my colleagues to support this 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 H.R. 6824, the President's Cup Cybersecurity Competition Act.

Mr. Speaker, you merely have to turn on the news to hear about the latest ransomware problem that continues to vex our country. According to research funded by the National Institute of Standards and Technology, there is a deficit of almost half a million cybersecurity employees in the U.S. Now more than ever, it is critical that the Federal Government provide cybersecurity education and pathways to Federal employment and make Federal retention of this limited skill set a priority.

One very important effort is underpinned by the President's Cup Cybersecurity Competition Act. CISA launched the first President's Cup Cybersecurity Act in 2019, as a national cybersecurity competition for both individuals and teams, aiming to identify, challenge, and reward the best cybersecurity talent in the Federal workforce.

This bill grants CISA the authority to fully implement the cybersecurity competition with certain parameters and provide prizes to winning individuals and teams. By codifying the cybersecurity competition, we further incentivize a skilled cybersecurity workforce. We also signal that Congress is committed to addressing Federal cybersecurity recruitment and retention challenges.

Mr. Speaker, I urge Members to join me in supporting H.R. 6824, and I yield back the balance of my time.

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

Mr. Speaker, the President's Cup Cybersecurity Competition has been an important part of our strategy to support a strong Federal cybersecurity workforce in recent years. Unfortunately, without congressional authorization, it lacks the stability it needs. So thanks to this legislation, authored by my committee colleague, Representative LURIA, we have the opportunity to authorize and preserve a key retention tool in the Federal toolbox to ensure that talented Federal cyber professionals get the recognition they deserve.

Mr. Speaker, I urge my colleagues to support H.R. 6824, and I yield back the balance of my time.

Mrs. LURIA. Mr. Speaker, a critical element of strengthening our nation's cybersecurity is ensuring the Federal government employs the best and the brightest with the most advanced cybersecurity skills.

Whether at CISA, our intelligence agencies, our military, or at other departments across the Federal government, cybersecurity professionals play an essential role in keeping our nation safe, and we must prioritize their recruitment, development, and retention.

Unfortunately, it has been challenging to compete with the private sector for cyber talent, so we must look to creative ways to strengthen the Federal cyber workforce.

The President's Cup Cybersecurity Competition is one innovative part of that effort.

Organized by CISA, this annual cybersecurity competition brings together cybersecurity professionals, both civilian and military, from across the Federal government to compete in a series of challenges that test a wide range of cybersecurity skills.

My legislation would authorize this competition to ensure it remains part of our Federal cyber workforce strategy and grants CISA the necessary authorities to fully carry out the program.

Importantly, it addresses legal barriers that have prevented CISA from directly providing cash prizes to winning teams and individuals that work in other departments or agencies.

H.R. 6824 specifically authorizes CISA to confer cash prizes to the winners, many of whom are in the military, for their achievement.

By passing this legislation, we demonstrate our commitment to further developing a competitive and highly skilled Federal cybersecurity workforce.

I thank Representatives CONNOLLY and GARBARINO for cosponsoring this bill, and Chairman THOMPSON and Ranking Member KATKO for their support for authorizing this important program.

I urge my colleagues to join me in supporting this bipartisan bill and look forward to working with them to get it enacted into law.

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.