In consideration of the substantial threats and attacks to nonprofit institutions by domestic and foreign terrorists and violent homegrown extremists, the vulnerability of nonprofits to destruction, incapacitation, or exploitation from a terrorist attack, and the challenges nonprofits face in providing for needed investments in target hardening and related preparedness activities, The Jewish Federations respectfully urges the Members of the Committee to support the ''Securing American Non-Profit Organizations Against Terrorism Act of 2019'' at markup.

Sincerely,

ROBERT B. GOLDBERG,
Senior Director, Legislative Affairs.

Miss RICE of New York. Mr. Speaker, I strongly encourage my colleagues to support H.R. 2476, and I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, H.R. 2476 would, for the first time, formally authorize the Department of Homeland Security's Nonprofit Security Grant Program.

This important grant program makes funding available to nonprofit organizations that are at risk of a terrorist attack.

Increasingly, nonprofit organizations throughout the United States and abroad have experienced an alarming increase in violence and threats of violence.

In just the first six months of 2019, the level of bloodshed in places of worship have shocked the world.

In addition to the April 27th shooting, where a gunman opened fire on congregants at a Passover celebration at a California synagogue, there was the April 21st coordinated terrorist attack on churches and hotels in Sri Lanka that killed nearly 250 people and the March 15th live-streamed mass shooting at a mosque in New Zealand, where 50 people were killed.

The horror of these attacks was compounded by the three church burnings in Louisiana in April.

Prior to this year, there were the 2018 ''Tree of Life'' synagogue shooting in Pittsburgh, where 11 people were killed; the 2017 Sutherland Springs, Texas church shooting, where 26 people were killed; and the 2012 shooting at a Sikh Temple in Milwaukee.

These attacks amplify the need for religious and other nonprofit organizations to have access to resources to keep themselves safe from bad actors.

Enactment of H.R. 2476 will help non-profits and places of worship take steps to be safer.

I introduced this legislation to authorize $75 million in grants with Representatives PETER KING (R–NY), MAX ROSE (D–NY), STEVE STIVERS (R–OH), BILL PASCRELL (D–NJ), and TROY BALDERSON (R–OH) in early May and, to date, it has over 100 Democrats and Republicans.

H.R. 2476 was endorsed by The Jewish Federations of North America.

I truly appreciate their support and commitment to this vital homeland security program.

Prospects for enactment of this legislation are good, as a bipartisan companion bill has been introduced.

Mr. Speaker, I urge support for H.R. 2476.

Ms. JACKSON LEE. Mr. Speaker, I rise in strong support of H.R. 2476, the ''Securing American Non-Profit Organizations Against Terrorism Act of 2019.''

H.R. 2476 reauthorizes the Department of Homeland Security's Nonprofit Security Grant Program (NSGP).

The bill would fund the NSGP at $75 million through fiscal year 2024; where $50 million would be reserved for nonprofit institutions located within UASI jurisdictions, and $25 million would be reserved for nonprofit institutions located outside of UASI jurisdictions.

This bill is caused by the recent increase in violence and threats of violence against nonprofit institutions.

Examples of such violence against nonprofit organizations include:

April 27—attack on the Poway synagogue that killed 11 April 21—a coordinated terrorist attack on churches and hotels in Sri Lanka that killed nearly 250 people and injured more than 500 people.

March 15—the deadly New Zealand mosque shootings, where 5o people were killed.

It is critical that we better understand the seriousness of such violent crimes as they impact not only the victims, but also their families, communities, and the generations of people to come.

This bill will allow the Nonprofit Security Grant Program to—Target activities, including physical security enhancement equipment, inspection and the screening systems.

Pay for security training relating to physical security and cybersecurity, target hardening, terrorism awareness, and employee awareness.

Along with, any other appropriate activity, including cybersecurity resilience activities, as determined by the Administrator.

When enacted, H.R. 2476 will create a better understanding on how we can manage and prevent terrorist acts towards non-profit organizations by targeting activities and increasing security training.

Mr. Speaker, I urge my colleagues to join me in supporting H.R. 2476 to confront such violence against nonprofit institutions, which pose as a strong threat to the citizens of the United States.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Miss RICE) that the House suspend the rules and pass the bill, H.R. 2476.

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

A motion to reconsider was laid on the table.

DHS CYBER INCIDENT RESPONSE TEAMS ACT OF 2019

Miss RICE of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1158) to authorize cyber incident response teams at 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. 1158

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''DHS Cyber Incident Response Teams Act of 2019''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBER INCIDENT RESPONSE TEAMS.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 148) is amended—

(1) in subsection (d)(1)(B)(iv), by inserting '', including cybersecurity specialists'' after ''entities'';

(2) by redesignating subsections (f) through (m) as subsections (g) through (n), respectively;

(3) by inserting after subsection (e) the following new subsection (f):

''(f) CYBER INCIDENT RESPONSE TEAMS.—

''(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

''(A) Assistance to asset owners and operators in restoring services following a cyber incident.

''(B) The identification of cybersecurity risk and unauthorized cyber activity.

''(C) Mitigation strategies to prevent, deter, and protect against cybersecurity risks.

''(D) Recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate.

''(E) Such other capabilities as the Under Secretary appointed under section 103(a)(1)(H) determines appropriate.

''(2) CYBERSECURITY SPECIALISTS.—The Secretary may include cybersecurity specialists from the private sector on cyber hunt and incident response teams.

''(3) ASSOCIATED METRICS.—The Center shall continually assess and evaluate the cyber incident response teams and their operations using robust metrics.

''(4) SUBMITTAL OF INFORMATION TO CONGRESS.—Upon the conclusion of each of the first four fiscal years ending after the date of the enactment of this subsection, the Center shall submit to the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate, information on the metrics used for evaluation and assessment of the cyber incident response teams and operations pursuant to paragraph (3), including the resources and staffing of such cyber incident response teams. Such information shall include each of the following for the period covered by the report:

''(A) The total number of incident response requests received.

''(B) The number of incident response tickets opened.

''(C) All interagency staffing of incident response teams.

''(D) The interagency collaborations established to support incident response teams.''; and

(4) in subsection (g), as redesignated by paragraph (2)—

(A) in paragraph (1), by inserting '', or any team or activity of the Center,'' after ''Center''; and

(B) in paragraph (2), by inserting '', or any team or activity of the Center,'' after ''Center''.

(b) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to be appropriated to carry out the requirements of this Act and the amendments made by this Act. Such requirements shall be carried out using amounts otherwise authorized to be appropriated.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Miss RICE) and the gentleman from Texas (Mr. CRENSHAW) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

□ 1530

GENERAL LEAVE

Miss RICE of New York. 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 gentlewoman from New York?

There was no objection.

Miss RICE of New York. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, every day, hackers grow bolder, more sophisticated, and more ambitious. In 2016, the Russian Government carried out an unprecedented attack on our election infrastructure; and last year, the Department of Homeland Security and FBI revealed that the Russians were exploiting cyber tools to target critical infrastructure in our energy, water, aviation, and commercial sectors.

Other foreign adversaries have taken note of Russia's activity and are similarly leveraging their cyber capabilities to advance their interests and undermine our own. We already know that Chinese actors have been targeting American companies and even our transportation systems with cutting-edge cyberattacks. In recent years, we have also seen an increase in Iranian cyberattacks on banks, businesses, and government agencies.

Meanwhile, local governments across the country, from Atlanta to Baltimore to Albany, have been devastated by costly and disruptive ransomware attacks.

The only way for us to effectively mitigate and respond to these attacks is by leveraging the full power and capabilities of the Federal Government.

H.R. 1158, the DHS Cyber Incident Response Teams Act of 2019, would do just that by authorizing hunt and incident response teams.

Housed within the Cybersecurity and Infrastructure Security Agency, these teams deploy to owners and operators of critical infrastructure after a cybersecurity incident. They provide intrusion analysis, identify malicious actors, analyze malicious tools, and provide mitigation assistance strategies. They are our boots on the ground in the event of a cybersecurity incident and are critical to improving the cybersecurity capabilities of critical infrastructure operators.

Additionally, H.R. 1158 authorizes DHS to leverage private-sector capabilities to address these growing and evolving threats.

It is important that DHS use every measure available to confront the changing landscape of cyber threats. Passing this bill, authored by our former chairman of the Homeland Security Committee, MIKE MCCAUL, will help us accomplish that mission.

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

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

I rise today in support of H.R. 1158, the DHS Cyber Incident Response Teams Act of 2019.

H.R. 1158 authorizes cyber hunt and incident response teams to assist operators, free of cost, to identify unauthorized cyber activity while promoting the proper strategies to deter future threats.

This legislation helps us stay vigilant in our efforts to respond to cyber incidents in both the public and private sectors as threats to our digital networks continue to evolve.

I support this important bill, introduced by my colleague, Ranking Member MCCAUL, and I commend him for his leadership on this issue. I urge all Members to support this bill.

Mr. Speaker, I reserve the balance of my time.

Miss RICE of New York. Mr. Speaker, I have no more speakers, and I am prepared to close after the gentleman from Texas closes.

I reserve the balance of my time.

Mr. CRENSHAW. Mr. Speaker, I yield 5 minutes to the gentleman from Texas (Mr. MCCAUL).

Mr. MCCAUL. Mr. Speaker, I rise today in support of my bill, H.R. 1158, the DHS Cyber Incident Response Teams Act of 2019. I want to thank the gentleman from Texas for managing this on the floor. I want to thank the gentlewoman from New York for her comments.

Every day, we are facing threats from Russia, China, Iran, North Korea, and other malicious actors trying to hit not only our Federal Government networks, but our private sector.

During my time as chairman of the House Homeland Security Committee, I prioritized ensuring that our Nation had the capacity to respond to cyber threats and protect our critical infrastructure. I am proud to say that we have made important strides in recent years, including standing up the Cybersecurity and Infrastructure Security Agency within DHS.

However, we must press forward with innovative solutions to respond to a constantly changing threat landscape. To that end, my bill authorizes CISA's ability to maintain cyber incident response teams to assist against cyberattacks on the government and private sector. These teams not only help respond to cyberattacks, but also help mitigate the potential destruction they cause and restore damaged networks after.

Additionally, my bill allows for leading industry specialists to serve on these teams with the government and DHS to provide outside expertise. It really provides a force multiplier, and I think it is a very important step forward in the right direction. It ensures that we have the best and brightest from both the public and private sector working in unison to secure our critical infrastructure and vital national networks.

These response teams are a force multiplier, enhancing our cybersecurity workforce and helping protect our interconnected world. This bill is critical to keeping our digital networks and communications systems resilient and protected.

I would like to also thank Congressmen LANGEVIN, RATCLIFFE, RUPPERSBERGER, and KATKO for joining me in introducing this bill.

This bill actually passed the House last Congress, and I sure hope we can get it passed by the Senate and signed into law, because it is urgently needed by the Department to protect the United States from these critical cyberattacks.

Mr. Speaker, I urge support of this legislation.

Mr. CRENSHAW. Mr. Speaker, I urge adoption of the bill, and I yield back the balance of my time.

Miss RICE of New York. Mr. Speaker, I yield myself such time as I may consume.

It is hard to predict the future, but there is one thing I know: Our adversaries will continue to hone their hacking capabilities to advance their interests and undermine ours.

Critical infrastructure owners and operators must have access to the incident response capabilities necessary to protect their networks. H.R. 1158, which was approved unanimously in committee, will help ensure that DHS can continue to partner effectively with the private sector to protect critical infrastructure.

Before I close, I would like to note that a version of this bill passed the House by a voice vote in the 115th Congress. I urge my colleagues to support H.R. 1158.

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

Ms. JACKSON LEE. Mr. Speaker, I rise in strong support of H.R. 1158, ''DHS Cyber Incident Response Teams Act of 2019.''

H.R. 1158 codifies DHS' National Cybersecurity and Communications Coordination Center (NCCIC) Hunt and Incident Response Teams which the Department currently deploys to provide intrusion analysis, identify malicious actors, analyze malicious tools, and provide mitigation assistance to entities requesting assistance after a cybersecurity incident.

H.R. 1158 also requires the NCCIC to submit information to Congress regarding metrics for the teams, at the end of the first four years after enactment.

In 2017, a malware named NotPetya was released from the hacked servers of a Ukrainian software firm servicing a management program used by some of world's largest corporations, causing an estimated $10 billion in damage.

When this bill passes, it will assess and mitigate situations of cyberterrorism that undermine our nation's security and civil liberties such as our national elections.

Cyber threats are becoming more sophisticated every day.

Due to the vulnerability of corporations' operations, we need extensive measures to identify, analyze, and alleviate threats of cyberattacks.

Affected asset owners and operators will receive critical information to improve their overall network and control systems security to lower cybersecurity risks, and other recommendations.

Mr. Speaker, I urge my colleagues to join me in supporting H.R. 1158 to protect our nation from malicious attempts of cyberterrorism that strategically weaken our democracy.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Miss RICE) that the House suspend the rules and pass the bill, H.R. 1158, 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.

STRENGTHENING LOCAL TRANSPORTATION SECURITY CAPABILITIES ACT OF 2019

Miss RICE of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2539) to require the Secretary of Homeland Security to prioritize the assignment of certain officers and intelligence analysts from the Transportation Security Administration and the Office of Intelligence and Analysis of the Department of Homeland Security to locations with participating State, local, and regional fusion centers in jurisdictions with a high-risk surface transportation asset in order to enhance the security of such assets, including by improving timely sharing of classified information regarding terrorist and other threats, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2539

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 Local Transportation Security Capabilities Act of 2019''.

SEC. 2. DEFINITIONS.

In this Act:

(1) PUBLIC AND PRIVATE SECTOR STAKEHOLDERS.—The term ''public and private sector stakeholders'' has the meaning given such term in section 114(u)(1)(C) of title 49, United States Code.

(2) SURFACE TRANSPORTATION ASSET.—The term ''surface transportation asset'' includes facilities, equipment, or systems used to provide transportation services by—

(A) a public transportation agency (as such term is defined in section 1402(5) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53; 6 U.S.C. 1131(5)));

(B) a railroad carrier (as such term is defined in section 20102(3) of title 49, United States Code);

(C) an owner or operator of—

(i) an entity offering scheduled, fixed-route transportation services by over-the-road bus (as such term is defined in section 1501(4) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53; 6 U.S.C. 1151(4))); or

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

SEC. 3. THREAT INFORMATION SHARING.

(a) PRIORITIZATION.—The Secretary of Homeland Security shall prioritize the assignment of officers and intelligence analysts under section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h) from the Transportation Security Administration and, as appropriate, from the Office of Intelligence and Analysis of the Department of Homeland Security, to locations with participating State, local, and regional fusion centers in jurisdictions with a high-risk surface transportation asset in order to enhance the security of such assets, including by improving timely sharing of classified information regarding terrorist and other threats.

(b) INTELLIGENCE PRODUCTS.—Officers and intelligence analysts assigned to locations with participating State, local, and regional fusion centers under this section shall participate in the generation and dissemination of transportation security intelligence products, with an emphasis on terrorist and other threats to surface transportation assets that—

(1) assist State, local, and Tribal law enforcement agencies in deploying their resources, including personnel, most efficiently to help detect, prevent, investigate, apprehend, and respond to terrorist and other threats;

(2) promote more consistent and timely sharing of threat information among jurisdictions; and

(3) enhance the Department of Homeland Security's situational awareness of such terrorist and other threats.

(c) CLEARANCES.—The Secretary of Homeland Security shall make available to appropriate owners and operators of surface transportation assets, and to any other person that the Secretary determines appropriate to foster greater sharing of classified information relating to terrorist and other threats to surface transportation assets, the process of application for security clearances under Executive Order No. 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or any successor Executive order.

SEC. 4. LOCAL LAW ENFORCEMENT SECURITY TRAINING.

(a) IN GENERAL.—The Secretary of Homeland Security, in consultation with public and private sector stakeholders, may develop, through the Federal Law Enforcement Training Centers, a training program to enhance the protection, preparedness, and response capabilities of law enforcement agencies with respect to terrorist and other threats at a surface transportation asset.

(b) REQUIREMENTS.—If the Secretary of Homeland Security develops the training program described in subsection (a), such training program shall—

(1) be informed by current information regarding terrorist tactics;

(2) include tactical instruction tailored to the diverse nature of the surface transportation asset operational environment; and

(3) prioritize training officers from law enforcement agencies that are eligible for or receive grants under sections 2003 or 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605) and officers employed by railroad carriers that operate passenger service, including interstate passenger service.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Miss RICE) and the gentleman from Texas (Mr. CRENSHAW) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Miss RICE of New York. 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 gentlewoman from New York?

There was no objection.

Miss RICE of New York. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 2539, the Strengthening Local Transportation Security Capabilities Act of 2019.

Every day, tens of millions of Americans rely on our Nation's vast transportation surface system. Securing that system must remain one of our top national security priorities.

H.R. 2539 will help bolster situational awareness about threats to these vital systems by requiring DHS to prioritize the assignment of officers and intelligence analysts to State, local, and regional fusion centers located in areas with high-risk surface transportation assets.

Further, H.R. 2539 authorizes a training program to enhance the effectiveness of law enforcement agencies that protect surface transportation assets.

I would like to thank my colleague, Ms. BARRAGÁN, for introducing this important bill. I urge my House colleagues to support H.R. 2539.

Mr. Speaker, I reserve the balance of my time.

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

I rise today in support of H.R. 2539, the Strengthening Local Transportation Security Capabilities Act of 2019. This bill will provide important support to surface transportation security at a time when our transportation sector faces evolving threats.

This bill ensures that the Secretary of Homeland Security will prioritize the assignment of intelligence analysts to fusion centers in areas with high-risk surface transportation assets to bolster security, improve coordination, and enhance information sharing.

This bill underscores the critically important work of State, local, and regional fusion centers in protecting the homeland. These centers analyze current threats and push critical threat information to the front lines.

It is important that Congress pass bills like this to strengthen the relationships among Federal, State, and local jurisdictions so that relevant threat information reaches the right people in a timely manner.

I am pleased by the support of my Democratic colleagues for fusion centers and hope this will lead to quick