

The bill includes vital civil rights and civil liberties safeguards to protect First Amendment rights.

The first step in confronting a threat is making sure that the people on the front lines have the information they need to understand it.

When it comes to the white supremacist threat, that is exactly what this bill would do.

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

□ 1315

Mr. JOYCE of Pennsylvania. Mr. Speaker, I yield myself such time as I may consume.

I rise today in strong support of H.R. 5736, the Transnational White Supremacist Extremism Review Act.

H.R. 5736 requires the Department of Homeland Security Undersecretary for Intelligence and Analysis, I&A, to coordinate with Federal partners and develop a terrorism threat assessment concerning homeland threats related to “foreign violent white supremacist extremist organizations.”

This bill further requires I&A to share the information with State and local law enforcement partners, as well as fusion centers. Ensuring that State and local law enforcement and fusion centers have access to information on current and emerging threats is a fundamental responsibility of the Department of Homeland Security, particularly the Office of Intelligence and Analysis.

The Trump administration has taken significant action to address domestic extremism, including white supremacy. The creation of the Office of Targeted Violence and Terrorism Prevention in April 2019 and the release of the DHS Strategic Framework for Countering Terrorism and Targeted Violence in September 2019 demonstrate a coordinated and comprehensive commitment to addressing emerging threats in both international and domestic terrorism.

Subcommittee Ranking Member WALKER led our efforts to negotiate changes to the base bill during the committee markup. I want to thank Subcommittee Chairman ROSE for accepting our changes to the bill. I urge its passage, and I reserve the balance of my time.

Ms. UNDERWOOD. Mr. Speaker, I yield as much time as he may consume to the gentleman from New York (Mr. ROSE), the sponsor of this bill.

Mr. ROSE of New York. Mr. Speaker, I thank the gentlewoman from Illinois for yielding her time.

Mr. Speaker, I rise in support of my bill, H.R. 5736, the Transnational White Supremacist Review Act.

Today, our country faces a wide range of complex threats to our safety, our security, and our way of life. Not only are American families having to keep their communities safe and their economy together in the face of COVID, but in large swaths of the country, they are doing so while deal-

ing with more frequent and catastrophic natural disasters.

Sadly, though, amidst all of this, terrorism does not stop. The homeland security threat posed by white supremacist extremists is pervasive and persistent. Extremists exploit such crises as we are in right now. Often, this involves the targeting of the most vulnerable in society.

Earlier this year, the Directors of the FBI and the National Counterterrorism Center testified before our committee regarding the unrelenting nature of bad actors during times like these. Both testified to the significant homeland security threat posed by racially motivated domestic actors, primarily white supremacist extremists.

In my capacity as chair of the Intelligence and Counterterrorism Subcommittee, I have joined with my colleagues to raise the alarm about this threat. In carrying out my work on the committee, I have identified a common theme. And that is, plain and simple, that this white supremacist domestic terrorist problem is, in fact, not domestic at all. It is global in nature.

Look no further than the deadly attacks in El Paso, Texas, and Poway, California, last year. The U.S. experienced firsthand the ramifications of an international white supremacist movement when two domestic actors independently drew inspiration from the foreign terrorists who committed the Christchurch, New Zealand, attack.

Troublingly, there are reports that white supremacist groups have adapted recruitment tactics and begun using training camps modeled after jihadist groups like al-Qaida and ISIS.

Just last week, a former Trump administration counterterrorism official confirmed that training by foreign groups is happening when she acknowledged that there have been instances when our foreign counterterrorism partners have alerted us to the fact that U.S. citizens were in their countries to conduct trainings or participate in trainings with white supremacist movements.

These foreign partners told this former official that the U.S. is an exporter of this ideology and must address this problem.

This is exactly what this bill today seeks to address, a bill designed to send a message to our foreign partners that Congress hears them and is taking action.

This bill would require DHS to produce and circulate a threat assessment on foreign violent white supremacist extremist groups to local law enforcement. It would also push social media companies to do so much more in addressing this threat. Crucially, this bill includes civil rights and civil liberty safeguards as well.

Countering white supremacy will require a whole-of-society approach, education, awareness, and so on.

Through our work on this committee, we found that Americans stay safest when law enforcement at all lev-

els is equipped with the best available information. This bill makes sure that our frontline responders in the law enforcement community have just that.

It is endorsed by the ADL, an expert advocacy group that has tracked the white supremacist threat for decades. It is also endorsed by the Blue Dog Coalition, a group that looks past partisanship and advocates for common-sense national security solutions.

Mr. Speaker, I urge my colleagues to vote “yes” on its passage.

Mr. JOYCE of Pennsylvania. Mr. Speaker, I urge a “yes” vote on the bill, and I yield back the balance of my time.

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

As the surge in white supremacist extremist attacks in the United States and around world puts all of us at risk, I commend my committee colleague Mr. ROSE for introducing this legislation, and I urge passage.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Illinois (Ms. UNDERWOOD) that the House suspend the rules and pass the bill, H.R. 5736, 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.

SAFE COMMUNITIES ACT OF 2020

Ms. UNDERWOOD. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5780) to enhance stakeholder outreach to and operational engagement with owners and operators of critical infrastructure and other relevant stakeholders by the Cybersecurity and Infrastructure Security Agency to bolster security against acts of terrorism and other homeland security threats, including by maintaining a clearinghouse of security guidance, best practices, and other voluntary content developed by the Agency or aggregated from trusted sources, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5780

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 “Safe Communities Act of 2020”.

SEC. 2. RESPONSIBILITIES OF CISA DIRECTOR RELATING TO SECURITY RESOURCES CLEARINGHOUSE.

Subsection (c) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

(1) by redesignating paragraphs (6) through (11) as paragraphs (7) through (12), respectively; and

(2) by inserting after paragraph (5) the following new paragraph:

“(6) maintain a clearinghouse for owners and operators of critical infrastructure and other relevant stakeholders to access security guidance, best practices, and other voluntary content developed by the Agency in a manner consistent with the requirements of section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and the Plain Writing Act of 2010 (5 U.S.C. note) or aggregated from trusted sources;”.

SEC. 3. STAKEHOLDER OUTREACH AND OPERATIONAL ENGAGEMENT STRATEGY.

(a) STRATEGY.—Not later than 180 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall issue a strategy to improve stakeholder outreach and operational engagement that includes the Agency’s strategic and operational goals and priorities for carrying out stakeholder engagement activities.

(b) CONTENTS.—The stakeholder outreach and operational engagement strategy issued under subsection (a) shall include the following:

(1) A catalogue of the stakeholder engagement activities and services delivered by protective security advisors and cybersecurity advisors of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, including the locations of the stakeholder engagement and services delivered and the critical infrastructure sectors (as such term is defined in section 2001(3) of the Homeland Security Act of 2002 (6 U.S.C. 601(3)) involved.

(2) An assessment of the capacity of programs of the Agency to deploy protective security advisors and cybersecurity advisors, including the adequacy of such advisors to meet service requests and the ability of such advisors to engage with and deliver services to stakeholders in urban, suburban, and rural areas.

(3) Long-term objectives of the protective security advisor and cybersecurity advisor programs, including cross-training of the protective security advisor and cybersecurity advisor workforce to optimize the capabilities of such programs and capacity goals.

(4) A description of programs, policies, and activities used to carry out such stakeholder engagement activities and services under paragraph (1).

(5) Resources and personnel necessary to effectively support critical infrastructure owners and operators and, as appropriate, other entities, including non-profit organizations, based on current and projected demand for Agency services.

(6) Guidance on how outreach to critical infrastructure owners and operators in a region should be prioritized.

(7) Plans to ensure that stakeholder engagement field personnel of the Agency have a clear understanding of expectations for engagement within each critical infrastructure sector and subsector, whether during steady state or surge capacity.

(8) Metrics for measuring the effectiveness of stakeholder engagement activities and services under paragraph (1), including mechanisms to track regional engagement of field personnel of the Agency with critical infrastructure owners and operators, and how frequently such engagement takes place.

(9) Plans for awareness campaigns to familiarize owners and operators of critical infrastructure with security resources and support offered by the Cybersecurity and Infrastructure Security Agency, including the clearinghouse maintained pursuant to paragraph (6) of section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)), as added by section 2.

(10) A description of how to prioritize engagement with critical infrastructure sectors based on threat information and the capacity of such sectors to mitigate such threats.

(c) STAKEHOLDER INPUT.—In issuing the stakeholder outreach and operational engagement strategy required under subsection (a), the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall, to the extent practicable, solicit input from stakeholders representing the following:

(1) Each of the critical infrastructure sectors.

(2) Critical infrastructure owners and operators located in each region in which the Agency maintains a field office.

(d) IMPLEMENTATION PLAN.—Not later than 90 days after issuing the stakeholder outreach and operational engagement strategy required under subsection (a), the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks for protective security advisor and cybersecurity advisor workforce development, training, and retention plans.

(2) Projected timelines, benchmarks, and resource requirements for such tasks.

(3) Metrics to evaluate the performance of such tasks.

(e) CONGRESSIONAL OVERSIGHT.—Upon issuance of the implementation plan required under subsection (d), the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the stakeholder outreach and operational engagement strategy required under subsection (a) and the implementation plan required under subsection (b), together with any other associated legislative or budgetary proposals relating thereto.

SEC. 4. INFORMATION PROVIDED BY PROTECTIVE SECURITY ADVISORS.

The Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall ensure, to the greatest extent practicable, protective security advisors of the Agency are disseminating homeland security information on voluntary programs and services of the Department of Homeland Security, including regarding the Nonprofit Security Grant Program, to bolster security and terrorism resilience.

SEC. 5. PROTECTIVE SECURITY ADVISOR FORCE MULTIPLIER PILOT PROGRAM.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall establish a one-year pilot program for State, local, Tribal, and territorial law enforcement agencies and appropriate government officials to be trained by protective security advisors of the Agency regarding carrying out security vulnerability or terrorism risk assessments of facilities.

(b) REPORT.—Not later than 90 days after the completion of the pilot program under subsection (a), the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall report on such pilot program to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from

Illinois (Ms. UNDERWOOD) and the gentleman from Pennsylvania (Mr. JOYCE) each will control 20 minutes.

The Chair recognizes the gentlewoman from Illinois.

GENERAL LEAVE

Ms. UNDERWOOD. 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 Illinois?

There was no objection.

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

Mr. Speaker, I rise today in strong support of H.R. 5780, the Safe Communities Act.

Last month, a teenager from my district in Antioch, Illinois, went to Kenosha, Wisconsin, where he allegedly killed two people with an AR-15-style rifle.

The next day, I heard from another constituent, a mother who lives in the alleged shooter’s hometown. She wrote: “There is a militia cell in Antioch that is becoming more and more emboldened to take the law into their own hands. I am becoming fearful to send my children to the same schools at white supremacist militia members.”

I share my constituents’ concerns with the rise of domestic violent extremism in this country. FBI Director Wray recently testified before the House Homeland Security Committee that white supremacist extremists are a leading threat to our Nation.

I believe we must do more to address the root causes of violent behavior, and I look forward to continuing to work with my colleagues in Congress to make America a place where racism, misogyny, and other forms of hate can no longer flourish.

Meanwhile, in the face of extremist threats like these, we must take immediate action to secure our critical infrastructure and make soft targets less vulnerable to attack.

In addition to domestic extremists, our suburban and rural communities face too many other threats of mass violence. Just last year, five of our neighbors, four of whom were my constituents, were killed by an act of gun violence at the Henry Pratt Company in Aurora, Illinois. Our workplaces, schools, and places of worship are far too vulnerable to mass shootings and other forms of targeted violence. This bill seeks to fix that.

Rural and suburban communities like mine in northern Illinois are increasingly targets of violence but often don’t have access to the Federal resources they need to protect themselves. That is why I introduced H.R. 5780, the Safe Communities Act of 2020, bipartisan legislation to help better protect soft targets in communities like mine.

The Cybersecurity and Infrastructure Security Agency's protective security advisers help improve security at schools, places of worship, and other soft targets, but there are too few of them to meet the demand of their services.

H.R. 5780 would require CISA to maintain an online security resources clearinghouse to provide security guidance and best practices, serving as a one-stop shop for school districts, religious organizations, and local officials to find the information they need to keep their communities safe.

The bill would also require CISA to develop a stakeholder outreach and operational engagement strategy and implementation plan to ensure that the Agency is delivering infrastructure security services across sectors and throughout regions.

Finally, H.R. 5780 would authorize a PSA force multiplier pilot program, which would require CISA PSAs to train State, local, Tribal, and territorial officials to perform security vulnerability and terrorism risk assessments. These risk assessments are an important part of qualifying for FEMA's security grants; the force multiplier program will help expand access to them.

I am proud that the Safe Communities Act of 2020 has been endorsed by the Jewish Federations of North America and the Anti-Defamation League.

I would like to thank my colleague, Mr. KATKO, for joining me in introducing this measure. I am grateful for his collaboration and leadership as ranking member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.

I want to extend my sincere appreciation to the Homeland Security Committee staff for their work on this legislation.

I urge my colleagues on both sides of the aisle to support this legislation today to make sure every community in America has the resources it needs to keep people safe.

I urge my colleagues to support H.R. 5780, and I reserve the balance of my time.

Mr. JOYCE of Pennsylvania. Mr. Speaker, I yield myself such time as I may consume.

I rise in support of H.R. 5780. This bill makes the great work done by the Cybersecurity and Infrastructure Security Agency more accessible to stakeholders.

CISA provides advice and recommendations upon the request of critical infrastructure owners and operators on how to secure and protect their facilities in cyberspace and physically.

This bill will help stakeholders clearly know what CISA can do. Continuing to develop the relationship between CISA and our private stakeholders remains an integral piece of our critical infrastructure security.

I thank Representatives UNDERWOOD and KATKO for their bill.

Mr. Speaker, I urge a "yes" vote on the bill, and I yield back the balance of my time.

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

Last week, I was appointed as the new chair of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Homeland Security Committee. It is a great honor and opportunity for me to amplify the homeland security concerns of the people of Illinois' 14th Congressional District here in Washington.

□ 1330

My constituents are concerned about the vulnerability of so-called soft targets to violence. CISA, which is overseen by my subcommittee, has a critical role to play to empower communities to be more secure and resilient against ever-increasing lists of homeland security threats.

I am committed to ensuring the success of the PSA program, and I look forward to working with CISA to make sure that every community can benefit from it. Enactment of the Safe Communities Act of 2020 will help CISA think more strategically about how it deploys PSAs and other services and do so in a way that will scale.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Illinois (Ms. UNDERWOOD) that the House suspend the rules and pass the bill, H.R. 5780, 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.

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

Ms. UNDERWOOD. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5823) to establish a program to make grants to States to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5823

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 Cybersecurity Improvement Act".

SEC. 2. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

(a) IN GENERAL.—Subtitle A of 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 sections:

"SEC. 2215. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

"(a) ESTABLISHMENT.—The Secretary, acting through the Director, shall establish a program to make grants to States to address

cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments (referred to as the 'State and Local Cybersecurity Grant Program' in this section).

"(b) BASELINE REQUIREMENTS.—A grant awarded under this section shall be used in compliance with the following:

"(1) The Cybersecurity Plan required under subsection (d) and approved pursuant to subsection (g).

"(2) The Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments required in accordance with section 2210, when issued.

"(c) ADMINISTRATION.—The State and Local Cybersecurity Grant Program shall be administered in the same program office that administers grants made under sections 2003 and 2004.

"(d) ELIGIBILITY.—

"(1) IN GENERAL.—A State applying for a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary a Cybersecurity Plan for approval. Such plan shall—

"(A) incorporate, to the extent practicable, any existing plans of such State to protect against cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments;

"(B) describe, to the extent practicable, how such State shall—

"(i) enhance the preparation, response, and resiliency of information systems owned or operated by such State or, if appropriate, by local, Tribal, or territorial governments, against cybersecurity risks and cybersecurity threats;

"(ii) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats in information systems of such State, local, Tribal, or territorial governments;

"(iii) ensure that State, local, Tribal, and territorial governments that own or operate information systems within the State adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology;

"(iv) promote the delivery of safe, recognizable, and trustworthy online services by State, local, Tribal, and territorial governments, including through the use of the .gov internet domain;

"(v) mitigate any identified gaps in the State, local, Tribal, or territorial government cybersecurity workforces, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, Tribal, and territorial government personnel to address cybersecurity risks and cybersecurity threats;

"(vi) ensure continuity of communications and data networks within such State between such State and local, Tribal, and territorial governments that own or operate information systems within such State in the event of an incident involving such communications or data networks within such State;

"(vii) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats related to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within such State;

"(viii) enhance capability to share cyber threat indicators and related information between such State and local, Tribal, and territorial governments that own or operate information systems within such State; and