I

116TH CONGRESS
2D SESSION

H. R. 5667

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.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 24, 2020

Ms. UNDERWOOD (for herself and Mr. KATKO) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

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.

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''.

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 the stakeholder engagement activities described in paragraphs (6) and (11) of section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)), as added and redesignated, respectively, by section 2 of this Act.

(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 other entities, as appropriate, 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.

(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 Sen-

ate 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.

○