116TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
116–476

SAFE COMMUNITIES ACT OF 2020

AUGUST 14, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 5780]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred 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, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

99–006

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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.

PURPOSE AND SUMMARY

H.R. 5780, the "Safe Communities Act of 2020" seeks to enhance the Cybersecurity and Infrastructure Security Agency's (CISA) capacity to carry out cybersecurity and infrastructure security activities in a manner that addresses the high demand and limited availability of Protective Security Advisor (PSA) and Cybersecurity Advisor (CSAs) services. H.R. 5780 would improve the availability of infrastructure security content online, ensure the smart regional deployment of CISA's infrastructure security resources, and leverage local law enforcement and government officials as force multipliers for cybersecurity and infrastructure security efforts. Specifically, H.R. 5780 directs CISA to maintain and make an online Security Resources Clearinghouse available to critical infrastructure owners and operators. The Security Resources Clearinghouse would include security guidance, best practices, and other voluntary content developed by CISA and other trusted sources. Additionally, H.R. 5780 would require CISA to develop a strategy to ensure that infrastructure security services are delivered across sectors and throughout regions. The strategy would also require CISA regional employees to educate stakeholders regarding the availability of other related security resources at the Department of Homeland

Security (DHS), including the Non-Profit Security Grant Program. Finally, the bill authorizes a PSA Force Multiplier Pilot Program in which CISA would be required to train State, local, Tribal, and territorial law enforcement agencies' employees and appropriate government officials to perform security vulnerability and terrorism risk assessments.

BACKGROUND AND NEED FOR LEGISLATION

In recent years, the country has experienced an increasing number of violent attacks at places of worship and other soft targets. According to the FBI, crimes against churches, synagogues, temples, and mosques increased almost 35 percent between 2014 and 2018. In mid-December 2019, the Department of Homeland Security's (DHS) Advisory Council warned that faith-based communities continued to be vulnerable to "extremist violence" and many in Congress were urging DHS and other Federal agencies to do more to protect them. At the same time, soft targets from shopping malls and movie theaters to schools and government office buildings continue to attract bad actors with violent goals.[1]

CISA works to improve the security of critical infrastructure—including places of worship and other soft targets—through the deployment of PSAs and CSAs. PSAs engage with critical infrastructure owners and operators to secure and mitigate vulnerabilities to critical infrastructure, including by providing vulnerability assessments of critical infrastructure assets. CSAs work to improve the cybersecurity posture of critical infrastructure owners and operators and facilitate improved coordination with the Federal government. Additionally, CISA provides certain curated resources online to help critical infrastructure owners and operators better secure their assets.

CISA's PSA/CSA program, together with its online resources, provide important security support to owners and operators of soft targets. That said, budget constraints and inconsistent efforts across critical infrastructure sectors, among other things, have limited CISA's capacity to provide guidance and support to all private sector partners that would benefit from its assistance. Demand for PSA and CSA services exceeds resources, as there are only 116 PSAs (about two per State) and about 80 CSAs (50 of which were newly funded in FY 2020). Moreover, CISA has been slow to grow a full complement of online resources to supplement services across critical infrastructure sectors. For instance, although CISA recently launched the Federal School Safety Clearinghouse, it does not maintain a similar clearinghouse for any other critical infrastructure sector.

In recognition of the fact that demand for PSA and CSA services far exceed those staffing levels, H.R. 5780 takes a holistic approach to expanding the delivery of security services to critical infrastructure owners and operators. It establishes new avenues to more effectively partner with infrastructure owners and operators by directing the broadening of the clearinghouse maintained by CISA beyond school administrators and officials to all critical infrastruc-

[1] "Homeland Security Experts on the Biggest Threats and Challenges the U.S. Faces in 2020," *Homeland Security Today* (Jan. 28, 2020), https://www.hstoday.us/subject-matter-areas/airport-aviation-security/homeland-security-experts-on-the-biggest-threats-and-challenges-the-u-s-faces-in-2020/.

ture sectors. It authorizes a force multiplier pilot to equip more State and local officials with the tools to partner with local infrastructure owners and operators to carry out vulnerability assessments. Additionally, the bill requires the CISA Director to develop a Stakeholder Engagement and Outreach Strategy and Implementation Plan to ensure that CISA effectively leverages the good work of PSAs and CSAs to improve the security of critical infrastructure.

HEARINGS

For the purposes of section 103(i) of H. Res. 6 of the 116th Congress, the following hearings were used to develop H.R. 5780:

- On January 9, 2020, the Committee held a hearing entitled "Understanding the Importance of DHS Preparedness Grants: Perspectives from the Field." The Committee received testimony form W. Greg Kierce, Director, Jersey City Office of Emergency Management and Homeland Security; Michael A. Sprayberry, Director, North Carolina Emergency Management, North Carolina Office of Recovery and Resiliency; Michael G. Masters, National Director and CEI, Secure Community Network; John J. Miller, Deputy Commissioner, Intelligence and Counterterrorism, New York City Police Department.
- On September 10, 2019, the Committee held a hearing entitled "Global Terrorism: Threats to the Homeland, Part I." The Committee received testimony from Peter Bergin, Vice President, Global Studies & Fellows, New America; Ali Soufan, Founder, The Soufan Center; Brian Levin, Director, Center for the Study of Hate & Extremism, California State University, San Bernardino; and Thomas Joscelyn, Senior Fellow, Foundation for the Defense of Democracies.

COMMITTEE CONSIDERATION

The Committee met on February 12, 2020, with a quorum being present, to consider H.R. 5780 and ordered the measure to be reported to the House with a favorable recommendation, with an amendment, by unanimous consent.

The following amendment was offered and agreed to by unanimous consent:

An amendment offered by Ms. Underwood.

Page 4, line 15, strike "and other entities, as appropriate," and insert "and, as appropriate, other entities, including non-profit organizations,".

Page 5, beginning line 15, insert the following: (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.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 5780.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 9, 2020.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5780, the Safe Communities Act of 2020.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 5780, Safe Communities Act of 2020
As ordered reported by the House Committee on Homeland Security on February 12, 2020

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	19	not estimated

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

H.R. 5780 would require the Cybersecurity and Infrastructure Security Agency (CISA) to provide information and guidance on securing critical infrastructure (such as power generation and transmission facilities) to state, local, and private stakeholders. CBO expects that, under the bill, CISA would provide that information on an agency website to help nonfederal entities protect themselves and their systems from terrorist threats. On the basis of information from CISA regarding similar information sharing programs, CBO estimates that it would cost $6 million in 2021 to develop and disseminate security guidance, training modules, and fact sheets. CBO expects that the department would need 13 new employees by 2022, at an average salary of $150,000, to communicate with the critical infrastructure community and to review additional materials for the website. In total, satisfying that requirement would cost $14 million over the 2020–2025 period, CBO estimates.

The bill also would authorize CISA to train state and local officials to assess risks to critical infrastructure through a one-year pilot program. Using information on the costs of similar training efforts, CBO estimates that it would cost $5 million to develop the curriculum and materials for the pilot program. If CISA chose to continue the pilot program after one year, costs would be higher than CBO estimates.

Satisfying the bill's reporting requirements would cost less than $500,000 over the 2020–2025 period.

For this estimate, CBO assumes that the bill will be enacted in fiscal year 2020. Under that assumption, CISA could incur some costs in 2020, but CBO expects that most of the costs would be incurred in 2021 and later. In total, CBO estimates that implementing H.R. 5780 would cost $19 million over the 2020–2025 period (see Table 1). Such spending would be subject to the availability of appropriations.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 5780

	By fiscal year, millions of dollars—						
	2020	2021	2022	2023	2024	2025	2020–2025
Security Resources Website:							
Estimated Authorization	*	6	2	2	2	2	14
Estimated Outlays	*	6	2	2	2	2	14
Train-the-Trainer Pilot Program:							
Estimated Authorization	*	5	0	0	0	0	5
Estimated Outlays	*	5	*	0	0	0	5
Total Changes:							
Estimated Authorization	*	11	2	2	2	2	19
Estimated Outlays	*	11	2	2	2	2	19

* = between zero and $500,000.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 5780 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the objective of H.R. 5780 is to improve the manner in which CISA delivers security services for critical infrastructure owners and operators, particularly places of worship and other soft targets. Toward that end, H.R. 5780 requires the CISA Director to establish a web-based clearinghouse of security guidance, best practices, and other voluntary content developed by CISA or aggregated from trusted sources. Additionally, the bill requires the CISA Director to develop a Stakeholder Outreach and Operational Engagement Strategy and Implementation Plan to improve the deployment of PSAs and CSAs. Finally, the bill requires CISA to launch a one-year pilot program whereby PSAs train appropriate State and local officials to perform risk and vulnerability assessments to create a force-multiplier to the overextended PSA workforce.

ADVISORY ON EARMARKS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section states that the Act may be cited as the "Safe Communities Act of 2020."

Sec. 2. Responsibilities of CISA director relating to security resources clearinghouse

This section requires the CISA Director to 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 CISA or aggregated from trusted sources. The content developed by CISA shall be done so 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). The Committee expects that CISA will, to the extent practicable and as appropriate, model the clearinghouse after a similar school security product, SchoolSafety.gov, which consolidates safety and security resources for education community stakeholders.[2] The clearinghouse should be designed as a

[2] SchoolSafety.gov was created by the Department of Homeland Security, the Department of Education, the Department of Justice, and the Department of Health and Human Services, through their work on the Federal Commission on School Safety. The clearinghouse "shares actionable recommendations to keep school communities safe" and "aims to help schools prevent, protect, mitigate, respond to, and recover from emergency situations." The portal offers security

user-friendly, accessible portal for a wide range of critical infrastructure stakeholders to access up-to-date security resources at scale.

Sec. 3. Stakeholder outreach and operational engagement strategy

This section requires the Director of CISA to develop a stakeholder outreach and engagement strategy within 180 days of enactment. The Committee anticipates that this strategy will help CISA make informed decisions about how to allocate limited PSA and CSA resources across all critical infrastructure owners and operators in a state or region. This strategy should address recent findings from the DHS Inspector General and the Government Accountability Office that highlight the challenges PSAs and CSAs encounter when trying to be responsive to targeted initiatives in certain sectors, such as the Election Security Initiative or the Hometown Security Initiative (focused on soft targets and crowded spaces), while also trying to ensure adequate coverage and support to all sectors.[3] These targeted initiatives are worthwhile, but may be placing additional strain on PSAs and CSAs to prioritize certain sectors at the expense of others. As such, the Committee expects that CISA will use the strategy development process to better understand PSA and CSA capacity, identify trade-offs in resource allocation, and establish clearer metrics to inform budget requests.

The strategy shall include: (1) a catalogue of stakeholder engagement activities and services provided by PSAs and CSAs; (2) an assessment of CISA's ability to deploy PSAs and CSAs, including to urban, suburban, and rural areas; (3) long-term objectives of the PSA and CSA program; (4) a description of the programs, policies, and activities used to carry out stakeholder engagement activities; (5) a description of resources and personnel necessary to support critical infrastructure owners and operators based on current and projected demands; (6) guidance on how outreach in a region should be prioritized; (7) plans to ensure that stakeholder engagement field personnel have a clear understanding of expectations for engagement within each critical infrastructure sector or subsector; (8) metrics for measuring the effectiveness of stakeholder engagement activities and services; (9) plans for awareness campaigns to familiarize owners and operators of critical infrastructure with the security resources and support offered by CISA, including the Security Resources Clearinghouse; and (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.

This section requires the CISA Director to engage with representatives from each of the critical infrastructure sectors from each CISA region in developing the stakeholder outreach and engagement strategy. Through this process, the Committee expects

---

assessment tools, guided resources to develop school security action plans, information on state programs and regional contacts for Federal agencies, and a platform for school security stakeholders to communicate with each other.

[3] See, e.g., DHS OIG–19–24, *Progress Made, But Additional Efforts are Needed to Secure the Election* (Feb. 28, 2019), https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf; GAO–20–267, *ELECTION SECURITY: DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections* (Feb. 2020), https://www.gao.gov/assets/710/704314.pdf; DHS OIG–20–37, *DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorism and Physical Threats* (Jun. 11, 2019), https://www.oig.dhs.gov/sites/default/files/assets/2020-06/OIG-20-37-Jun20.pdf.

that CISA will gain a better understanding of the needs within each sector and identify opportunities to improve CISA products and services to make them more responsive to such needs.

This section requires the CISA Director to issue an implementation plan 90 days after issuing the stakeholder outreach and engagement strategy defining: (1) strategic objectives and corresponding tasks for PSA and CSA workforce development, training, and retention plans; (2) projected timeline, benchmarks, and resource requirements for such tasks; and (3) metrics to evaluate the performance of such tasks.

This section requires the CISA Director to submit both the stakeholder outreach and engagement strategy and the implementation plan, along with associated legislative or budgetary proposals, to the appropriate Congressional Committees. The Committee anticipates that the strategy and implementation plan will help to inform Congressional oversight and identify potential resourcing issues.

Sec. 4. Information provided by protective security advisors

This section requires the CISA Director to ensure, to the greatest extent practicable, CISA protective security advisors 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. The Committee intends for CISA to use this opportunity to educate owners and operators—particularly in sectors where physical and cybersecurity culture operations are less mature and capabilities less robust—about the full suite of resources available to them.

Sec. 5. Protective security advisor force multiplier pilot program

This section requires the Director of CISA to establish a one-year pilot program for State, local, Tribal, and territorial law enforcement agencies and appropriate government officials to be trained by CISA protective security advisors regarding carrying out security vulnerability or terrorism risk assessments of facilities. The Committee expects that this pilot program will serve as a force multiplier for PSAs to engage in "train the trainer" efforts and other similar activities that will help to scale the expertise and capabilities of the PSA program across all levels of government.

This section requires the Director of CISA to submit a report to the appropriate Congressional Committees on the pilot program within 90 days of its completion.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) REDESIGNATION.—

(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the "Cybersecurity and Infrastructure Security Agency" (in this subtitle referred to as the "Agency").

(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) DIRECTOR.—

(1) IN GENERAL.—The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this subtitle referred to as the "Director"), who shall report to the Secretary.

(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of Cybersecurity and Infrastructure Security of the Department.

(c) RESPONSIBILITIES.—The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and

other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

(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;

[(6)] *(7)* develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

[(7)] *(8)* maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

[(8)] *(9)* develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

[(9)] *(10)* carry out emergency communications responsibilities, in accordance with title XVIII;

[(10)] *(11)* carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; and

[(11)] *(12)* carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of Cybersecurity and Infrastructure Security who shall—

(1) assist the Director in the management of the Agency; and

(2) report to the Director.

(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

(i) identify and assess the nature and scope of terrorist threats to the homeland;

(ii) detect and identify threats of terrorism against the United States; and

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastruc-

ture of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

(H) To disseminate, as appropriate, information analyzed by the Department within the Department to other Federal Government agencies with responsibilities relating to homeland security and to State, local, tribal, and territorial government agencies and private sector entities with those responsibilities in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law en-

forcement-related information, relating to threats of terrorism against the United States.

(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs.

(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

(3) STAFF.—

(A) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise

and experience to assist the Agency in discharging the responsibilities of the Agency under this section.

(B) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(C) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(4) DETAIL OF PERSONNEL.—

(A) IN GENERAL.—In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) AGENCIES.—The Federal agencies described in this subparagraph are—

(i) the Department of State;
(ii) the Central Intelligence Agency;
(iii) the Federal Bureau of Investigation;
(iv) the National Security Agency;
(v) the National Geospatial-Intelligence Agency;
(vi) the Defense Intelligence Agency;
(vii) Sector-Specific Agencies; and
(viii) any other agency of the Federal Government that the President considers appropriate.

(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(f) COMPOSITION.—The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Assistant Director.

(2) The Infrastructure Security Division, headed by an Assistant Director.

(3) The Emergency Communications Division under title XVIII, headed by an Assistant Director.

(g) CO-LOCATION.—

(1) IN GENERAL.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) COORDINATION.—When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) PRIVACY.—

(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974");

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date of enactment of this title, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector-Specific Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note; Public Law 114–94).

* * * * * * *

○