Calendar No. 194

116TH CONGRESS *1st Session*	SENATE	REPORT 116–90

STATE AND LOCAL GOVERNMENT CYBERSECURITY ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1846

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO PROVIDE FOR ENGAGEMENTS WITH STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS, AND FOR OTHER PURPOSES

SEPTEMBER 10, 2019.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
89–010 WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO III, *Chief Counsel*
ANDREW J. TIMM, *Professional Staff Member*
MICHAEL J.R. FLYNN, *Senior Counsel*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
JEFFERY D. ROTHBLUM, *Minority Fellow*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 194

116TH CONGRESS *1st Session* | SENATE | REPORT 116–90

STATE AND LOCAL GOVERNMENT CYBERSECURITY ACT OF 2019

SEPTEMBER 10, 2019.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 1846]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1846) to amend the Homeland Security Act of 2002 to provide for engagements with State, local, Tribal and territorial governments, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of S. 1846, the State and Local Cybersecurity Act of 2019, is to improve the cybersecurity posture of state, local, tribal, and territorial governments (SLTTs) through the coordination of activities with the Department of Homeland Security's (DHS or the Department) National Cybersecurity and Communications Integration Center (NCCIC). Specifically, this bill requires the NCCIC to coordinate with non-Federal entities, such as the Multi-State Information Sharing and Analysis Center (MS–ISAC), for the purpose

of engaging with SLTTs to conduct cybersecurity exercises, provide operational and technical cybersecurity training, and among other things, provide notifications of specific incidents and malware information. The bill also requires the NCCIC to work with senior Federal and non-Federal, state and local officials, including state and local Chief Information Officers and senior election officials, to ensure the effective implementation of information security processes and procedures.

The bill codifies the NCCIC's ability to provide, on a voluntary basis, operational and technical assistance to SLTT governments. The Department is also authorized to enter into cooperative agreements or contracts to carry out the responsibilities and coordination activities outlined in this bill. The Department is required to provide a report to Congress one year after enactment, and every two years thereafter on the status of cybersecurity measures in each state and the largest urban areas of the United States. Finally, S. 1846 authorizes DHS to establish a voluntary initiative to deploy technical or analytic capabilities or services that utilize classified cyber threat indicators or intelligence on unclassified, non-Federal entities' information systems to detect and prevent malicious traffic. DHS is required to provide a report to Congress on the status of this initiative one year after the enactment of this bill.

II. Background and the Need for Legislation

State and local governments are under siege by an unprecedented number of cyberattacks perpetrated by malicious actors and nation-state adversaries exploiting vulnerabilities in government-operated information systems and elections systems.[1] However, state and local governments often lack the resources and technical capabilities to identify malicious activity, and protect and secure their information systems from vulnerabilities that leave them susceptible to potentially crippling cyberattacks. In May 2019, the cybersecurity firm Recorded Future released a report in which it found that ransomware attacks—a type of cyberattack in which cyber criminals block a victim's access to their computer systems or data until the victim pays a monetary sum usually in some form of cryptocurrency—against state and local governments increased by 39 percent in 2018.[2] Many states and localities are faced with the difficult choice of paying the ransom or refusing to pay the hackers to decrypt their information systems. In May 2019, the city of Baltimore was attacked by a ransomware virus known as Robinhood, which affected the city's phone system and other electronically administered services, including billing services.[3] Rather than paying the $76,000 requested by the hackers, the city of Baltimore opted to decline the hackers' offer to decrypt the systems and

[1] Benjamin Freed, *State and Local Governments Urged to Beef up Ransomware Defense*, State Scoop (July 29, 2019), https://statescoop.com/state-local-government-urged-ransomware-defense/; Benjamin Freed, *Report: Ransomware Attacks Against State and Local Government Are on the Rise*, State Scoop (May 13, 2019), https://statescoop.com/report-ransomware-attacks-against-state-and-local-government-are-on-the-rise/.

[2] Allan Liska, *Early Findings: Review of State and Local Government Ransomware Attacks*, Recorded Future 2 (Apr. 2019), https://www.recordedfuture.com/state-local-government-ransomware-attacks/.

[3] Benjamin Freed, *Baltimore Approves $10 Million for Ransomware Recovery*, State Scoop (July 26, 2019), https://statescoop.com/baltimore-city-council-approves-10-million-ransomware-recovery/.

expects to spend an estimated $18 million to harden and protect the city's information technology infrastructure from future attacks.[4]

To help SLTTs protect their systems from ransomware and other cyberattacks, DHS's Cybersecurity and Infrastructure Security Agency and the MS–ISAC, along with a number of other organizations, released a joint statement urging state and local governments to make cyber preparedness a priority by taking pre-emptive measures to secure their networks.[5] Moreover, in July 2019, the National Governors Association requested that its members develop robust cyber disruption response plans that account for, among other things, continuity of government in a disaster situation.[6] This follows Louisiana Governor John Bel Edwards' recent decision to declare a state of emergency following a series of ransomware attacks that disabled the computer systems of districts throughout the state.[7]

In the 115th Congress, to better understand the challenges Federal and SLTT governments face when protecting and securing information systems and networks from malicious cyberattacks, the Committee held a hearing on mitigating cybersecurity risks.[8] During the hearing, then-Assistant Secretary for the Office of Cybersecurity and Communications for the DHS's National Protection and Programs Directorate Jeanette Manfra noted that DHS "recognize[s] that there is a significant technology deficit across state and local governments, and State and local election systems, in particular."[9] She also testified that in response to Russian information operations during the 2016 election, DHS is "leading the interagency effort to provide voluntary assistance to State and local officials" to defend election infrastructure.[10] At the same hearing, Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs at the John F. Kennedy School of Government Affairs at Harvard University, testified that "States simply are not equipped to face . . . cyber attacks from nation-state adversaries who are spending billions of dollars and dedicating thousands of cyber operators to advance their national interests."[11]

S. 1846 strengthens the SLTT governments' ability to mitigate cybersecurity threats by leveraging established information sharing and coordination mechanisms within the Federal government, such as the NCCIC. In 2013, to clarify public and private sector responsibilities in cybersecurity, the President issued Presidential Policy Directive 21, which established cybersecurity as a "shared responsi-

---

[4] *Id.*

[5] *CISA, MS–ISAC, NGA & NASCIO Recommend Immediate Action To Safeguard Against Ransomware Attacks*, https://www.nascio.org/Portals/0/Ransomware%20Statement.pdf (last visited July 30, 2019).

[6] *State Cyber Disruption Response Plans*, Nat'l Governors' Assc. (July 2019), https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf.

[7] La. Proc. No. 115 JBE 2019 (July 24, 2019), http://gov.louisiana.gov/assets/EmergencyProclamations/115-JBE-2019-State-of-Emergency-Cybersecurity-Incident.pdf.

[8] *Mitigating America's Cybersecurity Risk: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 115th Cong. 62 (2018) (testimony of Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office), https://www.govinfo.gov/content/pkg/CHRG-115shrg32454/pdf/CHRG-115shrg32454.pdf.

[9] *Id.*

[10] *Id.*

[11] *Id.*

bility among the [SLTT] entities." [12] In 2014, Congress formally authorized the NCCIC in the National Cybersecurity Protection Act of 2014.[13] In 2015, Congress further defined the NCCIC's role in the Cybersecurity Act of 2015, by tasking the NCCIC with sharing cyber threat indicators, coordinating information exchange across the Federal Government, and providing information and recommendations on security and resilience to Federal and non-Federal entities.[14] Currently, the NCCIC functions as the principle civilian cybersecurity and communications entity for information-sharing across the SLTT governments, the Intelligence Community, law enforcement, and international entities.[15]

The NCCIC shares information and coordinates activities through a variety of means, including via information sharing and analysis centers (ISACs). In 2010, DHS designated the MS–ISAC as the cybersecurity ISAC for SLTT governments; the MS–ISAC is the primary resource for disseminating threat information, education materials, and cyber support programs for those entities.[16] Since the 2010 designation, DHS has provided funding to the MS–ISAC.[17] Moreover, to better leverage and share threat information with SLTT governments, the MS–ISAC has assigned dedicated staff to the NCCIC's watch floor.[18] This enables the MS–ISAC to serve as the focal point for threat prevention, protection, response, and recovery for state-level cyber incidents.[19] As of September 2018, MS–ISAC membership exceeds 4,200 organizations and includes all 50 states.[20]

Since 2012, DHS has funded the MS–ISAC to conduct an annual self-assessment, which is delivered in the form of a report, to measure gaps and capabilities of SLTT governments' cybersecurity programs.[21] The self-assessment measures SLTT government respondents' maturity levels based on the functions defined in the National Institute of Standards and Technology's Cybersecurity Framework for Critical Infrastructure and divides respondents into three major categories: state, local, and tribal governments. The MS–ISAC's FY 2017 report determined that states are projected to achieve "the recommended minimum maturity across all functions in 2023" and local governments are expected to achieve minimum maturity 2024.[22] The report did not provide an estimate for the tribal government category attaining the minimum recommended maturity level, but noted that as a group, tribal governments declined across

---

[12] Press Release, The White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[13] National Cybersecurity Protection Act of 2014, Pub. L. No. 113–282, 128 Stat. 3066.

[14] National Cybersecurity Protection Act of 2014, Consolidated Appropriations Act, Pub. L. No. 114–113, 129 Stat. 2242 (2015), and Pub. L. No. 113–282, § 226, 128 Stat. 3067.

[15] Cybersecurity and Infrastructure Sec. Agency, Dep't of Homeland Sec., Department of Homeland Security Cybersecurity Support to Nonfederal Levels of Government: State, Local, Tribal, and Territorial Government Entities (2019), https://www.dhs.gov/sites/default/files/publications/cisa_-_dhs_cybersecurity_support_to_nonfederal_levels_of_government.pdf.

[16] Information Sharing and Awareness, Dep't of Homeland Sec., https://www.dhs.gov/cisa/information-sharing-and-awareness (last visited July 19, 2019).

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Cybersecurity and Infrastructure Sec. Agency, *supra* note 15, at 13.

[21] *Id.*

[22] Multi-State Info. Sharing & Analysis Ctr., Dep't of Homeland Sec., Nationwide Cybersecurity Review (2017), https://www.cisecurity.org/wp-content/uploads/2018/10/NCSR-2017-Final.pdf.

all functions by an average of 12 percent in comparison to the previous year.[23]

In June 2016, DHS's Homeland Security Advisory Council, Cybersecurity Subcommittee also published a report examining DHS's coordination efforts with SLTT entities, and provided findings and recommendations focused on evolving these relationships.[24] The report recommended DHS enhance its communication with SLTT governments on the availability of cybersecurity training focusing on political leadership. Additionally, the report recommended establishing stronger directives to ensure that all homeland security grant programs integrate cyber protections and cyber personnel recognizing that "by requiring that a percentage of grant funding be spent on cybersecurity, DHS could make meaningful steps in increasing cybersecurity protections in all new technology purchases."[25]

S. 1846, the State and Local Government Cybersecurity Act of 2019, allows the Secretary to award grants to and enter into cooperative agreements and contracts with states, local governments, and non-Federal entities. Additionally, the bill requires that the NCCIC, in coordination with Federal and non-Federal entities, such as the MS–ISAC, conduct exercises, provide operational and technical cybersecurity training to address cybersecurity risks or incidents, and provide, upon request, operational, technical, or material support to secure and ensure the resilience of Federal and non-Federal information and election systems.

Finally, the bill would allow the Secretary, at the voluntary request of the non-Federal entity, to deploy technical or analytic capabilities or services utilizing classified cyber threat indicators or intelligence to detect or prevent malicious network traffic on unclassified non-Federal information systems. This provision augments DHS's Enhanced Cybersecurity Services (ECS) program, which is an intrusion prevention capability offered by the Department.[26]

III. Legislative History

Ranking Member Peters (D–MI) introduced S. 1846 on June 13, 2019, with Senator Rob Portman (R–OH). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 1846 at a business meeting on June 19, 2019. During the business meeting, an amendment was offered by Senators Peters and Portman making technical changes. The Committee ordered the bill, as amended, reported favorably by voice vote *en bloc*. Senators present for both the vote on the amendment and the bill as amended were: Johnson, Portman, Paul, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

---

[23] *Id.* at 7.

[24] Homeland Sec. Advisory Council, Dep't of Homeland Sec., Final Report to the Cybersecurity Subcommittee: Part II—State, Local, Tribal & Territorial 1 (2016), https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_SLTT_FINAL_Report.pdf.

[25] *Id.* at 11.

[26] Cybersecurity and Infrastructure Sec. Agency, Enhanced Cybersecurity Services (ECS), https://www.dhs.gov/cisa/enhanced-cybersecurity-services-ecs (last visited Aug. 6, 2019).

IV. SECTION-BY-SECTION ANAYLSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section would establish the bill may be cited as the "State and Local Government Cybersecurity Act of 2019."

Section 2. Amendments to the Homeland Security Act of 2002

Paragraph (1) amends Subtitle A of title XXII of the Homeland Security Act of 2002 to broaden the definition of the term "entity" to include domestic or foreign-owned associations, corporations, including for-profit and nonprofits corporations, partnerships, proprietorships, organizations, institutions, establishments, or individuals who are legally able to enter into agreements or contracts with the United States.

Paragraph (2) allows the Secretary of the Department of Homeland Security (DHS) authority to make grants and enter into cooperative agreements or contracts with States, local governments, and other non-Federal entities to carry out the Secretary's responsibilities related to cybersecurity and infrastructure protection including providing assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings.

Paragraph (3) directs the National Cybersecurity and Communications Integration Center (NCCIC) to coordinate with Federal and non-Federal agencies, through such organizations as the Multi-State Information Sharing and Analysis Center, to conduct exercises, provide operational and technical training, and share cyber threat indicators, if requested. Paragraph (3) also directs the NCCIC to provide notifications on incident and malware information specific to their customers and residents; provide and periodically update cybersecurity resources, standards, and best practices and procedures related to information security; work with Federal and non-Federal officials, including State and local Chief Information Officers, senior election officials, and national associations to secure and ensure the resilience of Federal and non-Federal information systems, including election systems; provide operational and technical assistance to detect cybersecurity risks and incidents, including through the deployment and sustainment of cybersecurity technologies, if requested; assist in the development of policies and procedures for the coordinated vulnerability disclosures; ensure awareness at the State and local level of DHS resources on information security for civilian information systems; promote cybersecurity education and awareness through engagement.

Paragraph (3) also directs the Secretary to submit a report to the Senate Homeland Security and Governmental Affairs Committee and the House Homeland Security Committee on the status of cybersecurity measures in place and any gaps that exist in each State and the largest urban areas of the United States.

Paragraph (3) also authorizes the Secretary to establish an initiative to deploy capabilities or services using classified cyber threat indicators or intelligence to detect and prevent malicious traffic on unclassified non-Federal information systems. Participation in the initiative is voluntary and at the request of the non-Federal entity. This section also requires the Secretary to submit a report not later than one year after the establishment of the ini-

tiative containing an assessment of the status, the rate of participation, effectiveness, and recommendations for improvement of this program.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 19, 2019.

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1846, the State and Local Cybersecurity Act of 2019.

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.

S. 1846, State and Local Government Cybersecurity Act of 2019
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 19, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	31	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 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

No S. 1846 would authorize the Department of Homeland Security (DHS) to continue to coordinate with state and local governments to enhance the cybersecurity of their information systems.

Under the bill, the DHS National Cybersecurity and Communications Integration Center (NCCIC) would continue to provide assistance to state and local governments including conducting cybersecurity exercises, providing training, and notifying them of cybersecurity threats. The bill also would authorize DHS to implement an initiative to help state and local governments detect and prevent malicious network traffic on nonfederal information systems. Those governments could choose not to participate in that initiative.

The NCCIC is already performing most of the coordination activities authorized in S. 1846. Implementing the voluntary initiative would require hiring additional cybersecurity advisors, deploying sensors to nonfederal networks, and sharing classified information on cybersecurity threats with state and local partners. Using information from DHS, CBO expects that implementing the provision would require, on average, 15 full-time equivalent employees in each year beginning in 2020, at an average annual rate of about $150,000 per employee. On the basis of similar programs, CBO also expects that deploying sensors to state and local governments and sharing classified cybersecurity threats at an unclassified level would cost $20 million. In total, CBO estimates that enacting S. 1846 would cost $31 million over the 2019–2024 period (see Table 1). Such spending would be subject to availability of appropriated funds.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 1846

	By fiscal year, millions of dollars—						
	2019	2020	2021	2022	2023	2024	2019–2024
Estimated Authorization	0	21	1	3	3	4	32
Estimated Outlays	0	20	1	3	3	4	31

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

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the following 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 italic, 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. 2201. DEFINITIONS.

(1) * * *

* * * * * * *

(4) ENTITY.—The term "entity" shall include—

(A) an association, corporation, whether for-profit or nonprofit, partnership, proprietorship, organization, institution, establishment, or individual, whether domestically or foreign owned, that has the legal capacity to enter into agreements or contracts, assume obligations, incur and pay debts, sue and be sued in its own right in a court of competent jurisdiction in the United States, and to be held responsible for its actions;

(B) a governmental agency or other governmental entity, including State, local, Tribal, and territorial government entities; and

(C) the general public.

[(4)**]** *(5)* * * *

[(5)**]** *(6)* * * *

[(6)**]** *(7)* * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) * * *

(b) * * *

(c) RESPONSIBILITIES.—The Director shall—

(1) * * *

* * * * * * *

(10) 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) carry out the authority of the Secretary under subsection (e)(1)(R); and

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

* * * * * * *

(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) * * *

* * * * * * *

(R) To make grants to and enter into cooperative agreements or contracts with States, local governments, and other non-Federal entities as the Secretary determines necessary to carry out the responsibilities of the Secretary related to cybersecurity and infrastructure security under this Act and any other provision of law, including grants, cooperative agreements, and contracts that provide assistance

and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings.

* * * * * * *

SEC. 2209. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) * * *

(b) * * *

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) ** * *

* * * * * * *

(6) upon request, providing timely *operational and* technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation;

* * * * * * *

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

* * * * * * *

(E) an entity that collaborates with State and local government, *including an entity that collaborates with election officials,* on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

* * * * * * *

(n) COORDINATION ON CYBERSECURITY FOR FEDERAL AND NON-FEDERAL ENTITIES.—

(1) COORDINATION.—The Center shall, to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

(A) conduct exercises with Federal and non-Federal entities;

(B) provide operational and technical cybersecurity training related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents to Federal and non-Federal entities to address cybersecurity risks or incidents, with or without reimbursement;

(C) assist Federal and non-Federal entities, upon request, in sharing cyber threat indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government as well as among Federal and non-Federal entities, in order to increase situational awareness and help prevent incidents;

(D) provide notifications containing specific incident and malware information that may affect them or their customers and residents;

(E) provide and periodically update via a web portal and other means tools, products, resources, policies, guidelines, controls, and other cybersecurity standards and best practices and procedures related to information security;

(F) work with senior Federal and non-Federal officials, including State and local Chief Information Officers, senior election officials, and through national associations, to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure and ensure the resiliency of Federal and non-Federal information systems and including election systems;

(G) provide, upon request, operational and technical assistance to Federal and non-Federal entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security, including by, as appropriate, deploying and sustaining cybersecurity technologies, such as an intrusion detection capability, to assist those Federal and non-Federal entities in detecting cybersecurity risks and incidents;

(H) assist Federal and non-Federal entities in developing policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry;

(I) ensure that Federal and non-Federal entities, as appropriate, are made aware of the tools, products, resources, policies, guidelines, controls, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of civilian information systems; and

(J) promote cybersecurity education and awareness through engagements with Federal and non-Federal entities.

(o) REPORT.—Not later than 1 year after the date of enactment of this subsection, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the status of cybersecurity measures that are in place, and any gaps that exist, in each State and in the largest urban areas of the United States.

(p) DEPLOYMENT OF ENHANCED CAPABILITIES.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this subsection, the Secretary may establish an initiative to enhance efforts to deploy technical or analytic capabilities or services that utilize classified threat indicators or intelligence for the purpose of detecting or preventing malicious network traffic on unclassified non-Federal information systems.

(2) VOLUNTARY PARTICIPATION.—Activities conducted under this subsection may only be carried out on a voluntary basis upon request of the non-Federal entity.

(3) REPORT.—Not later than 1 year after the date on which the Secretary establishes the initiative under this subsection, the Secretary shall submit to the Committee on Homeland Secu-

rity and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the initiative, which shall include—

(A) the status of the initiative;

(B) the rate of voluntary participation in the initiative;

(C) the effectiveness of the initiative; and (D) recommendations for expanding the use of classified cyber threat indicators to protect non-Federal entities.

○