**Calendar No. 458**

| 116TH CONGRESS *2d Session* | SENATE | REPORT 116–227 |
|---|---|---|

# CYBERSECURITY STATE COORDINATOR ACT OF 2020

## R E P O R T

OF THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

## S. 3207

TO REQUIRE THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO ESTABLISH A CYBERSECURITY STATE COORDINATOR IN EACH STATE, AND FOR OTHER PURPOSES

JUNE 1, 2020.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

99–010 WASHINGTON : 2020

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*
COLLEEN E. BERNY, *Professional Staff Member*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
JEFFREY D. ROTHBLUM, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

**Calendar No. 458**

116TH CONGRESS, *2d Session* | SENATE | REPORT 116–227

# CYBERSECURITY STATE COORDINATOR ACT OF 2020

JUNE 1, 2020.—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. 3207]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3207) to require the Director of the Cybersecurity and Infrastructure Security Agency to establish a Cybersecurity State Coordinator in each State, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS



## I. PURPOSE AND SUMMARY

S. 3207, the Cybersecurity State Coordinator Act of 2020, requires the Director of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to appoint a Cybersecurity State Coordinator in each state with appropriate qualifications and expertise. Each Cybersecurity State Coordinator is responsible for building Federal and non-Federal relationships; serving as a cybersecurity risk advisor to Federal and non-Federal entities; assisting in the sharing of cyber threat infor-

mation between Federal and non-Federal entities; and among other things, alerting non-Federal entities to available Federal resources. Each responsibility that involves a non-Federal entity is to be executed on a voluntary basis only if the non-Federal entity agrees.

The bill also requires the CISA Director to brief Congress within one year after the enactment of this bill, and again three years later, on the placement and efficacy of the Cybersecurity State Coordinators.

## II. Background and the Need for Legislation

Ransomware is an extremely prevalent threat technique for malicious actors, especially when targeting state, local, tribal, and territorial (SLTTs) governments.[1] In the first quarter of 2019 alone, new ransomware techniques increased attacks by 118 percent.[2] By August 2019, two-thirds of publicly-known ransomware attacks had targeted SLTT governments.[3] All told in 2019, "ransomware attacks . . . impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion."[4]

On February 11, 2020, the Committee held a hearing entitled, "What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity."[5] The purpose of the hearing was to examine how SLTT governments and U.S. critical infrastructure entities can mitigate and protect against persistent cybersecurity threats, with a focus on ransomware. During the hearing Amanda Crawford, Executive Director of the Texas Department of Information Resources, discussed how Texas was targeted by 50 known ransomware attacks last year.[6] This included a coordinated ransomware event in August 2019 that hit 23 municipal entities.[7] Incident responders included state government entities, private vendors, and the Federal Government, including DHS and the Federal Bureau of Investigation.[8] Ms. Crawford discussed the voluntary assistance CISA provided during the August 2019 ransomware event, including reverse engineering the malware.[9] Ms. Crawford lamented that there was miscommunication between

---

[1] Some examples of recent notable ransomware attacks include the 2017 global WannaCry attack, the 2018 attack against the city of Atlanta, and the 2019 attacks against the State of Texas and the cities of Baltimore and New Orleans. *See, e.g., What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity. Hearing before the S. Comm. on Homeland Sec. & Governmental Affairs*, 116th Cong. (2020) [hereinafter *What States, Locals and the Business Community Should Know and Do*] (testimony of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security).

[2] *McAfee Lab Threats Report 5*, McAfee (Aug. 2019), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

[3] StateScoop, *Report: Two-thirds of ransomware attacks in 2019 targeted state and local governments* (Aug. 28, 2019), https://statescoop.com/report-70-percent-of-ransomware-attacks-in-2019-hit-state-and-local-governments/.

[4] *The State of Ransomware in the US: Report and Statistics 2019*, EMSISOFT (Dec. 12, 2019), https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

[5] *What States, Locals and the Business Community Should Know and Do*, *supra* note 1.

[6] *Id*. (testimony of Amanda Crawford, Executive Director, Texas Department of Information Resources). *See also* Texas Dep't of Information Resources, *Ransomware and Incident Response in Texas* (Jan. 2020).

[7] Kate Fazzini, *Alarm in Texas as 23 towns hit by 'coordinated' ransomware attack*, CNBC (Aug. 19, 2019), https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html.

[8] Texas Dep't of Information Resources, *Ransomware and Incident Response in Texas* (Jan. 2020).

[9] *What States, Locals and the Business Community Should Know and Do*, *supra* note 1 (testimony of Amanda Crawford, Executive Director, Texas Department of Information Resources).

CISA and the state response efforts, which "primarily resulted from role confusion and a lack of clarity concerning what resources DHS–CISA could provide to help Texas."[10]

A key takeaway from the hearing was the need to deploy additional CISA resources to assist SLTT governments and U.S. critical infrastructure entities. According to CISA Director Christopher Krebs, CISA "must make it easier for our State and local partners to work with us in the Federal Government."[11] This includes "deploying additional dedicated risk advisors, State coordinators to the field with clear expectations on what services or assistance to expect from the Federal Government . . . ."[12] Krebs continued, "[o]ne of the things I want to make sure I have is a State and local dedicated resource in every State Capitol. I am under-invested in cyber advisors. I have to get more resources out in the field . . . ."[13] Christopher DeRusha, Chief Information Officer for the State of Michigan, agreed that having a dedicated state coordinator will ensure "greater continuity between efforts of State and Federal Government, [and] provide a stronger State voice within CISA, helping them better tailor their assistance to States and localities who have widely varying levels of maturity and needs."[14]

S. 3207 requires CISA to designate and deploy Cybersecurity State Coordinators to each state to ensure dedicated cybersecurity resources to, and clear communication with, SLTTs and non-Federal entities.

## III. LEGISLATIVE HISTORY

On January 16, 2020, Senator Margaret Wood Hassan (D–NH) introduced S. 3207, the Cybersecurity State Coordinator Act of 2020, which was referred to the Committee on Homeland Security and Governmental Affairs. Ranking Member Gary Peters (D–MI), Senator Rob Portman (R–OH), Senator John Cornyn (R–TX), Senator Jacky Rosen (D–NV), Senator Chris Van Hollen (D–MD), and Senator Kyrsten Sinema (D–AZ) are cosponsors.

The Committee considered S. 3207 at a business meeting on March 11, 2020. During the business meeting, Senator Hassan offered an amendment in the nature of a substitute. The Hassan Substitute Amendment added that the Cybersecurity State Coordinator must have appropriate cybersecurity qualifications and expertise; clarified that that the Cybersecurity State Coordinator is required to engage with non-Federal entities on a voluntary basis only; added that any additional duties performed by the Cybersecurity State Coordinator must be determined by the Director of CISA; clarified that the Director of CISA must consult with the relevant officials and entities regarding the appointment and performance of the Cybersecurity State Coordinator; required a briefing to Congress after one year and three years on the placement and efficacy of the Cybersecurity State Coordinators; and made additional technical changes.

---

[10] *Id.*

[11] *Id.* (testimony of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security).

[12] *Id.*

[13] *Id.*

[14] *Id.* (testimony of Christopher DeRusha, Chief Security Officer, Cybersecurity and Infrastructure Protection Office, State of Michigan).

The Committee favorably reported the bill *en bloc*, as amended by the Hassan Substitute Amendment, by voice vote. Senators present for the vote were: Johnson, Portman, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Harris, Sinema, and Rosen.

## IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

*Section 1. Short title*

This section provides the bill's short title, the "Cybersecurity State Coordinator Act of 2020."

*Section 2. Findings*

In this section, Congress finds that cyber threats to SLTT entities, such as ransomware, have drastically increased. SLTT entities face increased threats from a number of actors, including advanced persistent threats, hostile nation states, and cybercriminals. As a result, there is a pressing need for additional Federal coordination and knowledge to assist SLTT entities in increasing their resiliency against cyber threats. It is critical that Federal and non-Federal entities, including SLTT governments, Information Sharing and Analysis Centers, election officials, State adjutants general, and additional non-Federal entities coordinate to prevent, manage, and recover from cyberattacks.

*Section 3. Cybersecurity State Coordinator*

Section 3, subsection (a) adds a new section to the Homeland Security Act that authorizes the CISA Director to appoint a Cybersecurity State Coordinator in each state and describes the responsibilities of the Cybersecurity State Coordinators.

Subsection (a) of the new section authorizes the Director of CISA to appoint a Cybersecurity State Coordinator, with the appropriate qualifications and expertise, in each state. Subsection (b) of the new section outlines the duties of the Cybersecurity State Coordinator, which include: building Federal and voluntary non-Federal relationships; serving as a cybersecurity risk advisor to Federal, and non-Federal entities; assisting in the sharing of cyber threat information between Federal and non-Federal entities; alerting non-Federal entities to available financial, technical, and operational Federal resources; supporting training and exercises to expedite recovery in the event of a cyberattack; being a principal point of contact for non-Federal entities to engage with the Federal Government; assisting in the development and coordination of vulnerability disclosure programs for non-Federal entities; and performing additional duties as determined by the Director of CISA to manage cybersecurity risk. This section explicitly states that responsibilities vis-à-vis non-Federal entities are to be undertaken on a voluntary basis only. Subsection (c) of the new section requires the Director of CISA to consult with the relevant state and local officials regarding the appointment of the Cybersecurity State Coordinator within each state. This section also requires the Director of CISA to consult with the appropriate state and local officials, as well as non-Federal entities, on the performance of the Cybersecurity State Coordinator.

Section 3 subsection (b) requires the Director of CISA to brief Congress not later than one year and again three years after the date of enactment of this Act on the placement and efficacy of the Cybersecurity State Coordinators.

Section 3 subsection (c) provides a rule of construction that clarifies that nothing in this legislation shall be read to affect or modify the authority of Federal law enforcement to investigate cyber incidents.

Finally, section 3 subsection (d) provides a technical and conforming amendment to modify the Homeland Security Act of 2002's table of contents consistent with the new section added by this legislation.

## 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, March 31, 2020.*

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. 3207, the Cybersecurity State Coordinator 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.

**S. 3207, Cybersecurity State Coordinator Act of 2020**

**As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 11, 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) | * | 37 | 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.

S. 3207 would direct the Cybersecurity and Infrastructure Security Agency (CISA) to improve the capacity of state and local governments to protect against cybersecurity threats. The bill would require CISA to appoint a cybersecurity coordinator for each state. Those coordinators would help entities affected by malicious cyber activity access the financial, technical, and operational resources that are available from the federal government.

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. On the basis of information from CISA, CBO expects that the department would need 56 new employees to serve as cybersecurity coordinators at an average compensation of $179,000. After accounting for the time needed to appoint those coordinators and adjusting for inflation, implementing S. 3207 would cost $37 million over the 2020–2025 period, CBO estimates. Such spending would be subject to the availability of appropriations (see Table 1).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 3207

| | By fiscal year, millions of dollars— | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2020–2025 |
| Estimated Authorization | * | 1 | 4 | 9 | 11 | 12 | 37 |
| Estimated Outlays | * | 1 | 4 | 9 | 11 | 12 | 37 |

* = 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.

## 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, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted

is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

# HOMELAND SECURITY ACT OF 2002

* * * * * * *

**Section 1. Short Title; Table of Contents.**

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:



# TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

## Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

**SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.**

(a) * * *

(b) * * *

(c) * * *

(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) appoint a Cybersecurity State Coordinator in each State, as described in section 2215; and*

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

* * * * * * *

***SEC. 2215. CYBERSECURITY STATE COORDINATOR.***

*(a) APPOINTMENT.—Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifica-*

*tions and expertise, who shall serve as the Cybersecurity State Coordinator.*

*(b) DUTIES.—The duties of Cybersecurity State Coordinator appointed under subsection (a) shall include—*

*(1) building strategic relationships across Federal and, on a voluntary basis, non-Federal entities by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;*

*(2) serving as a Federal cybersecurity risk advisor and coordinating between Federal and, on a voluntary basis, non-Federal entities to support preparation, response, and remediation efforts relating to cybersecurity risks and incidents;*

*(3) facilitating the sharing of cyber threat information between Federal and, on a voluntary basis, non-Federal entities to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;*

*(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;*

*(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;*

*(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;*

*(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards; and*

*(8) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.*

*(c) FEEDBACK.—The Director shall consult with relevant State and local officials regarding the appointment, and State and local officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.*

*(d) OVERSIGHT.—The Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a briefing on the placement and efficacy of the Cybersecurity State Coordinators appointed under section 2215 of the Homeland Security Act of 2002, as added by subsection (a)—*

*(1) Not later than 1 year after the date of enactment of this Act; and*

*(2) Not later than 2 years after providing the first briefing under this subsection.*

*(e) RULE OF CONSTRUCTION.—Nothing in this section or the amendment made by this section shall be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents.*

○