IN THE CONGRESS OF THE UNITED STATES

JUNE 6, 2020

Mr. LEE (for himself, Mr. JACOB, Ms. KIKI, Mr. KRISHNA, and Mr. WATKINS) introduced the following bill;

A BILL

To require the Director of Cybersecurity and Infrastructure Security Agency to establish a Cybersecurity State Coordinator in each State, and for other purposes.

Be it enacted by the House of Representatives and Senate of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity State Coordinator Act of 2020".

SECTION 2. FINDINGS.

Congress finds that—

(1) cyber threats, such as ransomware, against State, local, Tribal, and territorial entities have grown at an alarming rate;

(2) State, local, Tribal, and territorial entities face a growing threat from advanced persistent actors, hostile nation states, criminal groups, and other malicious cyber actors;

(3) there is an urgent need for greater engagement and expertise from the Federal Government to help these entities build their resilience and defense; and

(4) coordination within Federal entities and between Federal and non-Federal entities, including State, local, Tribal, and territorial governments, Information Sharing and Analysis Centers, election officials, State adjutants general, and other non-Federal entities is critical to anticipating, preventing, managing, and recovering from cyberattacks.

SECTION 3. DEFINITIONS.

In this Act—

(a) CYBERSECURITY.— The term "cybersecurity" means measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

(b) CYBERSECURITY STATE COORDINATOR.— The term "cybersecurity state coordinator" means an individual appointed by the Director of Cybersecurity and Infrastructure Security Agency to each State.

(c) RANSOMWARE.— The term "ransomware" means malware that requires the victim to pay a ransom to access encrypted files.

SECTION 4. CYBERSECURITY STATE COORDINATOR.

(a) IN GENERAL.— Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2202(c) (6 U.S.C. 652(c))—

(A) in paragraph (10), by striking "and" at the end;

(B) by redesignating paragraph (11) as paragraph (12); and

(C) by inserting after paragraph (10) the following:

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

(2) by adding at the end the following:

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

(a) APPOINTMENT.— The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) DUTIES.— The duties of a 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, exercise, and planning for continuity of operations for 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."

(b) OVERSIGHT.— The Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Secretary of Security 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.

(c) RULE OF CONSTRUCTION.— Nothing in this section or the amendments 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.

(d) TECHNICAL AND CONFORMING AMENDMENT.— The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107-296; 116 Stat. 2135) is amended by inserting after the item relating to section 2214 the following:

"Sec. 2215. Cybersecurity State Coordinator.".

SECTION 5. ENACTMENT.

EFFECTIVE DATE.— The provisions of this Act shall come into force on January 1, 2021.

Written by Sec. of Security Lee (R-SC-3)

AUTHOR'S NOTES:

1. *This bill was inspired by S.3207 - Cybersecurity State Coordinator Act of 2020.*