117TH CONGRESS
1ST SESSION

S. 2407

To ensure timely Federal Government awareness of cyber intrusions that pose a threat to national security, enable the development of a common operating picture of national-level cyber threats, and to make appropriate, actionable cyber threat information available to the relevant government and private sector entities, as well as the public, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 21, 2021

Mr. WARNER (for himself, Mr. RUBIO, Ms. COLLINS, Mr. HEINRICH, Mr. TESTER, Mr. KING, Mr. BURR, Mr. BLUNT, Mr. BENNET, Mr. CASEY, Mr. SASSE, Mrs. GILLIBRAND, Mrs. FEINSTEIN, Mr. RISCH, and Mr. MANCHIN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To ensure timely Federal Government awareness of cyber intrusions that pose a threat to national security, enable the development of a common operating picture of national-level cyber threats, and to make appropriate, actionable cyber threat information available to the relevant government and private sector entities, as well as the public, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Incident Notification Act of 2021''.

SEC. 2. CYBERSECURITY INTRUSION REPORTING CAPABILITIES.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

''Subtitle C—Cybersecurity Intrusion Reporting Capabilities

''SEC. 2231. DEFINITIONS.

''In this subtitle:

''(1) DEFINITIONS FROM SECTION 2201.—The definitions in section 2201 shall apply to this subtitle, except as otherwise provided.

''(2) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Select Committee on Intelligence of the Senate;

''(C) the Committee on the Judiciary of the Senate;

''(D) the Committee on Armed Services of the Senate;

''(E) the Committee on Homeland Security of the House of Representatives;

''(F) the Permanent Select Committee on Intelligence of the House of Representatives;

''(G) the Committee on the Judiciary of the House of Representatives; and

''(H) the Committee on Armed Services of the House of Representatives.

''(4) COVERED ENTITY.—The term 'covered entity' has the meaning given the term under the rules required to be promulgated under section 2233(d).

''(5) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given the term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

''(6) CYBER INTRUSION REPORTING CAPABILITIES.—The term 'Cyber Intrusion Reporting Capabilities' means the cybersecurity intrusion reporting capabilities established under section 2232.

''(7) CYBERSECURITY NOTIFICATION.—The term 'cybersecurity notification' means a notification of a cybersecurity intrusion, as defined in accordance with section 2233.

''(8) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

''(9) FEDERAL AGENCY.—The term 'Federal agency' has the meaning given the term 'agency' in section 3502 of title 44, United States Code.

''(10) FEDERAL CONTRACTOR.—The term 'Federal contractor'—

''(A) means a contractor or subcontractor (at any tier) of the United States Government; and

''(B) does not include a contractor or subcontractor that holds only—

''(i) service contracts to provide housekeeping or custodial services; or

''(ii) contracts to provide products or services unrelated to information technology below the micro-purchase threshold (as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor thereto).

''(11) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40, United States Code.

''(12) RANSOMWARE.—The term 'ransomware' means any type of malicious software that prevents the legitimate owner or operator of an information system or network from accessing computer files, systems, or networks and demands the payment of a ransom for the return of such access.

"SEC. 2232. ESTABLISHMENT OF CYBERSECURITY INTRUSION REPORTING CAPABILITIES.

''(a) DESIGNATION.—The Agency shall be the designated agency within the Federal Government to receive cybersecurity notifications from other Federal agencies and covered entities in accordance with this subtitle.

''(b) ESTABLISHMENT.—Not later than 240 days after the date of enactment of this subtitle, the Director shall establish Cyber Intrusion Reporting Capabilities to facilitate the submission of timely, secure, and confidential cybersecurity notifications from Federal agencies and covered entities to the Agency.

''(c) RE-EVALUATION OF SECURITY.—The Director shall re-evaluate the security of the Cyber Intrusion Reporting Capabilities not less frequently than once every 2 years.

''(d) REQUIREMENTS.—The Cyber Intrusion Reporting Capabilities shall allow the Agency—

''(1) to accept classified submissions and notifications; and

''(2) to accept a cybersecurity notification from any entity, regardless of whether the entity is a covered entity.

''(e) LIMITATIONS ON USE OF INFORMATION.—Any cybersecurity notification submitted to the Agency through the Cyber Intrusion Reporting Capabilities established under this section—

''(1) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the ''Freedom of Information Act''), in accordance with subsection (b)(3)(B) of such section 552, and any State, Tribal, or local provision of law requiring disclosure of information or records; and

''(2) may not be—

''(A) admitted as evidence in any civil or criminal action brought against the victim of the cybersecurity incident, except for actions brought by the Federal Government under section 2233(h); or

''(B) subject to a subpoena, unless the subpoena is issued by Congress and necessary for congressional oversight purposes.

''(f) PRIVACY.—The Agency shall adopt privacy and data protection procedures, based on the comparable privacy and data protection procedures developed for information received and shared pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.), for information submitted to the Agency through the Cyber Intrusion Reporting Capabilities established under subsection (b) that is known at the time of sharing to contain personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(g) ANNUAL REPORTS.—

''(1) DIRECTOR REPORTING REQUIREMENT.—Not later than 1 year after the date on which the Cyber Intrusion Reporting Capabilities are established and once each year thereafter, the Director shall submit to the appropriate congressional committees a report, in classified form if necessary, on the number of notifications received through the Cyber Intrusion Reporting Capabilities, and a description of the associated mitigations taken, during the 1-year period preceding the report.

''(2) SECRETARY REPORTING REQUIREMENT.—Not later than 1 year after the date on which the Cyber Intrusion Reporting Capabilities are estab-

lished, and once each year thereafter, the Secretary shall submit to the appropriate congressional committees a report on—

"(A) the categories of covered entities, noting additions or removals of categories, that are required to submit cybersecurity notifications; and

"(B) the types of cybersecurity intrusions and other information required to be submitted as a cybersecurity notification, noting any changes from the previous submission.

"(3) FORM.—The annual reports required under this subsection may be submitted as a single report for each year, at the discretion of the Secretary.

"SEC. 2233. REQUIRED NOTIFICATIONS.

"(a) NOTIFICATIONS.—

"(1) IN GENERAL.—Except as provided in paragraph (2), not later than 24 hours after the confirmation of a cybersecurity intrusion or potential cybersecurity intrusion, the Federal agency or covered entity that discovered the cybersecurity intrusion or potential cybersecurity intrusion shall submit a cybersecurity notification to the Agency through the Cyber Intrusion Reporting Capabilities.

''(2) EXCEPTION.—If a Federal agency or covered entity required to submit a cybersecurity notification under paragraph (1) is subject to another Federal law, regulation, policy, or government contract requiring notification of a cybersecurity intrusion or potential cybersecurity intrusion to a Federal agency within less than 24 hours, the notification deadline required in the applicable law, regulation, or policy shall also apply to the notification required under this section.

''(b) REQUIRED UPDATES.—A Federal agency or covered entity that submits a cybersecurity notification under subsection (a) shall, until the date on which the cybersecurity incident is mitigated or any follow-up investigation is completed, submit updated cybersecurity threat information to the Agency through the Cyber Intrusion Reporting Capabilities not later than 72 hours after the discovery of new information.

''(c) REQUIRED CONTENTS.—The notification and required updates submitted under subsections (a) and (b) shall include, at minimum, any information required to be included pursuant to the rules promulgated under subsection (d).

''(d) REQUIRED RULEMAKING.—

''(1) IN GENERAL.—Notwithstanding any provisions set out in this title that may limit or restrict the promulgation of rules, and not later than 270 days after the date of enactment of this subtitle, the Secretary, acting through the Director, in coordination with the Director of National Intelligence, the Director of the Office of Management and Budget, the Secretary of Defense, and the National Cyber Director, shall promulgate interim final rules, waiving prior public notice, and accepting comments after the effective date in order to inform the final rules—

''(A) that define 'covered entity' for the purpose of identifying entities subject to the cybersecurity notification requirements of this section and which shall include, at a minimum, Federal contractors, owners or operators of critical infrastructure, as determined appropriate by the Director based on assessment of risks posed by compromise of critical infrastructure operation, and nongovernmental entities that provide cybersecurity incident response services;

''(B) that define 'cybersecurity intrusion' and 'potential cybersecurity intrusion' for the

purpose of determining when a cybersecurity notification shall be submitted under this section;

"(C) that define 'cybersecurity threat information' for the purpose of describing the threat information to be included in a cybersecurity notification under this section;

"(D) that define 'confirmation of a cybersecurity incident or potential cybersecurity incident' for the purpose of determining when a notification obligation is triggered;

"(E) that address whether a Federal agency or covered entity shall be required to provide a cybersecurity notification for a cybersecurity intrusion of which the Federal agency or covered entity is aware, but does not directly impact the networks or information systems owned or operated by the Federal agency or covered entity; and

"(F) that contain other provisions necessary to implement the requirements of this subtitle.

"(2) REQUIREMENTS FOR DEFINITIONS.—At a minimum, the definitions of 'cybersecurity intrusion' and 'potential cybersecurity intrusion' required to be

promulgated under paragraph (1)(B) shall include a cybersecurity intrusion, including an intrusion involving ransomware, that—

"(A) involves or is assessed to involve a nation-state;

"(B) involves or is assessed to involve an advanced persistent threat cyber actor;

"(C) involves or is assessed to involve a transnational organized crime group (as defined in section 36 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2708));

"(D) results, or has the potential to result, in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of people in the United States;

"(E) is or is likely to be of significant national consequence; or

"(F) is identified by covered entities but affects, or has the potential to affect, agency systems.

"(3) REQUIRED INFORMATION FOR CYBERSECURITY THREAT INFORMATION.—For purposes of the rules required to be promulgated under para-

graph (1)(B), the cybersecurity threat information required to be included in a cybersecurity notification shall include, at a minimum—

"(A) a description of the cybersecurity intrusion, including identification of the affected systems and networks that were, or are reasonably believed to have been, accessed by a cyber actor, and the estimated dates of when such an intrusion is believed to have occurred;

"(B) a description of the vulnerabilities leveraged, and tactics, techniques, and procedures used by the cyber actors to conduct the intrusion;

"(C) any information that could reasonably help identify the cyber actor, such as internet protocol addresses, domain name service information, or samples of malicious software; and

"(D) contact information, such as a telephone number or electronic mail address, that a Federal agency may use to contact the covered entity, either directly or through an authorized agent of the covered entity; and

"(E) actions taken to mitigate the intrusion.

''(4) REQUIRED CONSULTATION.—For purposes of the rules required to be promulgated under paragraph (1), the Secretary, acting through the Director, shall consult with appropriate private sector stakeholders, as determined by the Secretary, in coordination with the Director of National Intelligence, the Director of the Office of Management and Budget, the Secretary of Defense, and the National Cyber Director.

''(e) REQUIRED RESPONSE.—The Director shall develop and implement a process to respond to a Federal agency or covered entity that submits a cybersecurity notification under subsection (a) not later than 2 business days after the date on which the notification is submitted, which shall notify the entity as to whether the Director requires further information about the cybersecurity intrusion.

''(f) REQUIRED COORDINATION WITH SECTOR RISK MANAGEMENT OR OTHER REGULATORY AGENCIES.—The Secretary of Homeland Security, acting through the Director, in coordination with the head of each Sector Risk Management Agency and other Federal agencies, as determined appropriate by the Director, shall—

''(1) establish a set of reporting criteria for Sector Risk Management Agencies and other Fed-

eral agencies as identified by the Director to submit cybersecurity notifications regarding cybersecurity incidents affecting covered entities in their respective sectors or covered entities regulated by such Federal agencies to the Agency through the Cyber Intrusion Reporting Capabilities; and

''(2) take steps to harmonize the criteria described in paragraph (1) with the regulatory reporting requirements in effect on the date of enactment of this subtitle.

''(g) PROTECTION FROM LIABILITY.—No cause of action shall lie or be maintained in any court by any person or entity, other than the Federal Government pursuant to subsection (h) or any applicable law, against any covered entity due to the submission by that person or entity of a cybersecurity notification to the Agency through the Cyber Intrusion Reporting System, in conformance with this subtitle and the rules promulgated under subsection (d), and any such action shall be promptly dismissed.

''(h) ENFORCEMENT.—

''(1) IN GENERAL.—If, on the basis of any information, the Director determines that a covered entity has violated, or is in violation of, the requirements of this subtitle, including rules promulgated

under this subtitle, the Director may assess a civil penalty not to exceed 0.5 percent of the entity's gross revenue from the prior year for each day the violation continued or continues.

''(2) DETERMINATION OF AMOUNT.—The Director shall have the authority to reduce or otherwise modify the civil penalties assessed under paragraph (1) and may take into account mitigating or aggravating factors, including the nature, circumstances, extent, and gravity of the violations and, with respect to the covered entity, the covered entity's ability to pay, degree of culpability, and history of prior violations.

''(3) PROCEDURES.—The Director shall establish procedures for contesting civil penalties imposed under this section.

''(4) COVERED ENTITIES WITH FEDERAL GOVERNMENT CONTRACTS.—In addition to the penalties authorized under this subsection, if a covered entity with a Federal Government contract violates the requirements of this subtitle, including rules promulgated under this subtitle, the Administrator of the General Services Administration may assess additional available penalties, including removal from the Federal Contracting Schedule.

''(5) FEDERAL AGENCIES.—If a Federal agency violates the requirements of this subtitle, the violation shall be referred to the Inspector General for the agency, and shall be treated by the Inspector General for the agency as a matter of urgent concern.

''(i) EXEMPTION.—All information collection activities under sections 2232 and 2233 of this subtitle shall be exempt from the requirements of sections 3506(c), 3507, 3508, and 3509 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act').

''(j) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to supersede any reporting requirements under subchapter I of chapter 35 of title 44, United States Code.

"SEC. 2234. PRESERVATION OF INFORMATION.

''(a) IN GENERAL.—Not later than 60 days after the date of enactment of this subtitle, the Secretary, acting through the Director, in coordination with the Director of the Office of Management and Budget, shall promulgate rules for data preservation standards and requirements for Federal agencies and covered entities to assist with cybersecurity intrusion response and associated investigatory activities.

''(b) MINIMUM REQUIREMENTS.—The rules for data preservation promulgated under subsection (a) shall require, at a minimum, that a Federal agency or covered entity that submits a cybersecurity notification under this subtitle shall preserve all of the data designated for preservation under such rules.

''SEC. 2235. ANALYSIS OF CYBERSECURITY NOTIFICATIONS.

''(a) ANALYSIS.—

''(1) IN GENERAL.—The Secretary, acting through the Director, the Attorney General, and the Director of National Intelligence, shall jointly develop procedures for ensuring any cybersecurity notification submitted to the System is promptly and appropriately analyzed to—

''(A) determine the impact of the breach or intrusion on the national economy and national security;

''(B) identify the potential source or sources of the breach or intrusion;

''(C) recommend actions to mitigate the impact of the breach or intrusion; and

''(D) provide information on methods of securing the system or systems against future breaches or intrusions.

''(2) REQUIREMENT.—The procedures required to be developed under paragraph (1) shall include criteria for when rapid analysis, notification, or public dissemination is required.

''(3) AUTHORITY.—The Secretary, acting through the Director, the Attorney General, and the Director of National Intelligence may each designate employees within each respective agency who may search intelligence and law enforcement information for cyber threat intelligence information with a national security or public safety purpose, based on cybersecurity notifications received by the Agency through the Cyber Intrusion Reporting Capabilities, and consistent with the procedures developed under paragraph (1).

''(b) ANALYTIC PRODUCTION.—

''(1) IN GENERAL.—Not less frequently than once every 30 days, the Secretary, acting through the Director, the Attorney General, and the Director of National Intelligence shall produce a joint cyber threat intelligence report that characterizes the current cyber threat picture facing Federal agencies and covered entities.

''(2) REQUIREMENTS.—Each report required to be produced under paragraph (1)—

''(A) shall be in a form which may be made publicly available;

''(B) may include a classified annex, as necessary; and

''(C) shall, to the maximum extent practical, anonymize attribution information from cybersecurity notifications received through the Cyber Intrusion Reporting Capabilities.

''(3) AUTHORITY TO DECLASSIFY.—The Director of National Intelligence may declassify any analytic products, or portions thereof, produced under this section if such declassification is required to mitigate cyber threats facing the United States.''.

(b) TABLE OF CONTENTS.—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 adding at the end the following:

''Subtitle C—Cybersecurity Intrusion Reporting Capabilities

''Sec. 2231. Definitions.
''Sec. 2232. Establishment of cybersecurity intrusion reporting capabilities.
''Sec. 2233. Required notifications.
''Sec. 2234. Preservation of information.
''Sec. 2235. Analysis of cybersecurity notifications.''.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) by redesignating the second and third paragraphs (12) as paragraphs (14) and (15), respectively; and

(2) by inserting before paragraph (14), as so redesignated, the following:

''(13) carry out the responsibilities described in subtitle C relating to the cybersecurity intrusion reporting capabilities;''.

○