Calendar No. 633

117TH CONGRESS
2D SESSION

S. 2875

[Report No. 117–249]

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 28, 2021

Mr. PETERS (for himself, Mr. PORTMAN, Ms. SINEMA, and Mr. TILLIS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 13, 2022

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, 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 Reporting Act of 2021''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms ''covered cyber incident'', ''covered entity'', and ''cyber incident'' have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 3(b) of this Act.

(2) CYBER ATTACK; RANSOM PAYMENT; RANSOMWARE ATTACK.—The terms ''cyber attack'', ''ransom payment'', and ''ransomware attack'' have the meanings given those terms in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651), as amended by section 3(a) of this Act.

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

(4) INFORMATION SYSTEM; SECURITY VULNERABILITY.—The terms ''information system'' and ''security vulnerability'' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

SEC. 3. CYBER INCIDENT REPORTING.

(a) DEFINITIONS.—

(1) IN GENERAL.—Section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), and (6) as paragraphs (2), (4), (5), (7), (10), and (11), respectively;

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

"(1) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.";

(C) by inserting after paragraph (2), as so redesignated, the following:

"(3) CYBER ATTACK.—The term 'cyber attack' means the use of unauthorized or malicious code on an information system, or the use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, avail-

ability, or integrity of electronic data stored on, processed by, or transiting an information system.'';

(D) by inserting after paragraph (5), as so redesignated, the following:

''(6) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third-party data center.'';

(E) by inserting after paragraph (7), as so redesignated, the following:

''(8) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(9) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means a cyber attack that includes the threat of use of unauthorized or malicious code on an information system, or the threat of use of another digital mechanism such as a de-

nial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

''(B) does not include any such event where the demand for payment is made by a Federal Government entity, good-faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.''; and

(F) by adding at the end the following:

''(13) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber attack that allows an adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (such as information technology products), or services at any point during the life cycle.

''(14) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value

that functions as a medium of exchange, a unit of account, or a store of value.

''(15) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.''.

(2) CONFORMING AMENDMENT.—Section 9002(A)(7) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(a)(7)) is amended to read as follows:

''(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651).''.

(b) CYBER INCIDENT REPORTING.—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—Cyber Incident Reporting

''SEC. 2230. DEFINITIONS.

''(a) IN GENERAL.—Except as provided in subsection (b), the definitions under section 2201 shall apply to this subtitle.

''(b) ADDITIONAL DEFINITIONS.—In this subtitle:

"(1) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

"(2) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the interim final rule and final rule issued pursuant to section 2232.

"(3) COVERED ENTITY.—The term 'covered entity' means an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the interim final rule and final rule issued pursuant to section 2232.

"(4) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2209(a).

"(5) CYBER THREAT.—The term 'cyber threat'—

"(A) has the meaning given the term 'cybersecurity threat' in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501); and

‘‘(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

‘‘(6) CYBER THREAT INDICATOR; CYBERSECURITY PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL; SECURITY VULNERABILITY.—The terms ‘cyber threat indicator’, ‘cybersecurity purpose’, ‘defensive measure’, ‘Federal entity’, ‘information system’, ‘security control’, and ‘security vulnerability’ have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

‘‘(7) SMALL BUSINESS.—The term ‘small business’—

‘‘(A) means a business with fewer than 50 employees (determined on a full-time equivalent basis); and

‘‘(B) does not include—

‘‘(i) a business that is a covered entity; or

‘‘(ii) a business that holds a government contract, unless that contractor is a party only to—

‘‘(I) a service contract to provide housekeeping or custodial services; or

‘‘(II) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

‘‘SEC. 2231. CYBER INCIDENT REVIEW OFFICE.

‘‘(a) CYBER INCIDENT REVIEW OFFICE.—There is established in the Agency a Cyber Incident Review Office (in this section referred to as the ‘Office’) to receive, aggregate, and analyze reports related to covered cyber incidents submitted by covered entities in furtherance of the activities specified in subsection (c) of this section and sections 2202(e), 2203, and 2209(c) and any other authorized activity of the Director to enhance the situational awareness of cyber threats across critical infrastructure sectors.

‘‘(b) ACTIVITIES.—The Office shall, in furtherance of the activities specified in sections 2202(e), 2203, and 2209(c)—

‘‘(1) receive, aggregate, analyze, and secure, consistent with the requirements under the Cyberse-

curity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls and identify tactics, techniques, and procedures adversaries use to overcome those controls;

"(2) receive, aggregate, analyze, and secure reports related to ransom payments to identify tactics, techniques, and procedures, including identifying and tracking ransom payments utilizing virtual currencies, adversaries use to perpetuate ransomware attacks and facilitate ransom payments;

"(3) leverage information gathered about cybersecurity incidents to—

"(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers; and

"(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident re-

sponse firms, and security researchers, with timely, actionable, and anonymized reports of cyber attack campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures;

''(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

''(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a substantial cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of

those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

"(7) with respect to covered cyber incident reports under subsection (c) involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

"(8) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the reports required under subsection (c);

"(9) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransom attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

"(10) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other pri-

vate sector organizations, to the greatest extent practicable;

''(11) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Office; and

''(12) in accordance with section 2235, not later than 24 hours after receiving a covered cyber incident report or ransom payment report, share the reported information with appropriate Sector Risk Management Agencies and other appropriate agencies as determined by the Director of Office Management and Budget, in consultation with the Director and the National Cyber Director.

''(c) PERIODIC REPORTING.—Not later than 60 days after the effective date of the interim final rule required under section 2232(b)(1), and on the first day of each month thereafter, the Director, in consultation with the Attorney General and the Director of National Intelligence, shall submit to the National Cyber Director, the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the

minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report that characterizes the cyber threat facing Federal agencies and covered entities, including applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the report, which shall—

"(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

"(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

"(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

"(B) intelligence gaps that have, or currently are, impeding the ability to counter covered cyber incidents and ransomware threats;

"(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

"(4) be unclassified, but may include a classified annex.

"(d) ORGANIZATION.—The Director may organize the Office within the Agency as the Director deems appropriate, including harmonizing the functions of the Office with other authorized activities.

"SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

"(a) IN GENERAL.—

"(1) COVERED CYBER INCIDENT REPORTS.—A covered entity shall report a covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

"(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual or a small business, that makes a ransom payment as the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

"(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

"(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the interim final rule and final rule issued pursuant to subsection (b).

"(5) EXCEPTIONS.—

"(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the interim final rule and final rule issued pursuant to subsection (b).

"(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

"(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed according to the interim final rule and final rule issued pursuant to subsection (b).

"(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the interim final rule and the final rule issued pursuant to subsection (b), except that the requirements of paragraph (1) through (4) shall not be effective for a period for more than 18 months after the effective date of the interim final rule if the Director has not issued a final rule pursuant to subsection (b)(2).

"(b) RULEMAKING.—

"(1) INTERIM FINAL RULE.—Not later than 270 days after the date of enactment of this section, and after a 60-day consultative period, followed by a 90-day comment period with appropriate stakeholders, the Director, in consultation with Sector Risk Management Agencies and the heads of other Federal agencies, shall publish in the Federal Register an interim final rule to implement subsection (a).

"(2) FINAL RULE.—Not later than 1 year after publication of the interim final rule under paragraph (1), the Director shall publish a final rule to implement subsection (a).

"(3) SUBSEQUENT RULEMAKINGS.—Any rule to implement subsection (a) issued after publication of the final rule under paragraph (2), including a rule to amend or revise the final rule issued under paragraph (2), shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

"(c) ELEMENTS.—The interim final rule and final rule issued pursuant to subsection (b) shall be composed of the following elements:

‘‘(1) A clear description of the types of entities that constitute covered entities, based on—

‘‘(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

‘‘(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

‘‘(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

‘‘(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

‘‘(A) at a minimum, require the occurrence of—

‘‘(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or

network, or a serious impact on the safety and resiliency of operational systems and processes;

''(ii) a disruption of business or industrial operations due to a cyber incident; or

''(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

''(B) consider—

''(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

''(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

''(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

"(C) exclude—

"(i) any event where the cyber incident is perpetuated by a United States Government entity, good-faith security research, or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and

"(ii) the threat of disruption as extortion, as described in section 2201(8)(B).

"(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

"(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident.

"(A) A description of the covered cyber incident, including—

"(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

"(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

"(iii) the estimated date range of such incident; and

"(iv) the impact to the operations of the covered entity.

"(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

"(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

"(D) Where applicable, identification of the category or categories of information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

"(E) The name and, if applicable, taxpayer identification number or other unique identifier of the entity impacted by the covered cyber incident.

"(F) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission, and at the direction, of the covered entity to assist with compliance with the requirements of this subtitle.

"(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment.

~~"(A) A description of the ransomware attack, including the estimated date range of the attack.~~

~~"(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.~~

~~"(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.~~

~~"(D) The name and, if applicable, taxpayer identification number or other unique identifier of the entity that made the ransom payment.~~

~~"(E) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.~~

~~"(F) The date of the ransom payment.~~

"(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

"(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

"(I) The amount of the ransom payment.

"(J) A summary of the due diligence review required under subsection (c).

"(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

"(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

"(A) be established by the Director in consultation with the Council;

"(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing

and contents of any such reports to the maximum extent practicable; and

"(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

"(8) Procedures for—

"(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), which shall include, at a minimum, a concise, user-friendly web-based form;

"(B) the Office to carry out the enforcement provisions of section 2233, including with respect to the issuance of subpoenas and other aspects of noncompliance;

"(C) implementing the exceptions provided in subparagraphs (A), (B), and (D) of subsection (a)(5); and

"(D) anonymizing and safeguarding information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(d) THIRD-PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

"(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under subsection (a).

"(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

"(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

"(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity

of the responsibilities of the impacted entity regarding a due diligence review under subsection (c) and reporting ransom payments under this section.

''(c) DUE DILIGENCE REVIEW.—Before the date on which a covered entity, or an entity that would be required to submit a ransom payment report under this section if that entity makes a ransom payment, makes a ransom payment relating to a ransomware attack, the covered entity or entity shall conduct a due diligence review of alternatives to making the ransom payment, including an analysis of whether the covered entity or entity can recover from the ransomware attack through other means.

''(f) OUTREACH TO COVERED ENTITIES.—

''(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

''(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

"(A) An overview of the interim final rule and final rule issued pursuant to subsection (b).

"(B) An overview of mechanisms to submit to the Office covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

"(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

"(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

"(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

"(F) An overview of the privacy and civil liberties requirements in this subtitle.

"(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

‘‘(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

‘‘(B) information sharing and analysis organizations;

‘‘(C) trade associations;

‘‘(D) information sharing and analysis centers;

‘‘(E) sector coordinating councils; and

‘‘(F) any other entity as determined appropriate by the Director.

‘‘(g) EVALUATION OF STANDARDS.—

‘‘(1) IN GENERAL.—Before issuing the final rule pursuant to subsection (b)(2), the Director shall review the data collected by the Office, and in consultation with other appropriate entities, assess the effectiveness of the rule with respect to—

‘‘(A) the number of reports received;

‘‘(B) the utility of the reports received;

‘‘(C) the number of supplemental reports required to be submitted; and

‘‘(D) any other factor determined appropriate by the Director.

‘‘(2) SUBMISSION TO CONGRESS.—The Director 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 the results of the evaluation described in paragraph (1) and may thereafter, in accordance with the requirements under subsection (b), publish in the Federal Register a final rule implementing this section.

''(h) ORGANIZATION OF REPORTS.—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), the Director may reorganize and reformat the means by which covered cyber incident reports, ransom payment reports, and any other voluntarily offered information is submitted to the Office.

"SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

''(a) IN GENERAL.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

''(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required

to be included, but may enhance the situational awareness of cyber threats.

''(c) APPLICATION OF PROTECTIONS.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

''SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

''(a) PURPOSE.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

''(b) INITIAL REQUEST FOR INFORMATION.—

''(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursu-

ant to paragraph (1) or (2) of section 2231(b), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Office within 72 hours in accordance to section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

"(2) TREATMENT.—Information provided to the Office in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

"(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

"(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred.

"(2) CIVIL ACTION.—

"(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

"(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

"(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as a contempt of court.

"(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

"(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity with a Federal Government contract, grant, or cooperative agreement fails to comply with a subpoena issued under this subsection—

"(A) the Director may refer the matter to the Administrator of General Services; and

"(B) upon receiving a referral from the Director, the Administrator of General Services

may impose additional available penalties, including suspension or debarment.

''(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Director determines, based on the information provided in response to the subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide that information to the Attorney General or the appropriate regulator, who may use that information for a regulatory enforcement action or criminal prosecution.

''(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Office by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

"(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

"(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

"(1) the size and complexity of the entity;

"(2) the complexity in determining if a covered cyber incident has occurred;

"(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments; and

"(4) for non-covered entities required to submit a ransom payment report, the ability of the entity to perform a due diligence review pursuant to section 2232(c).

"(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

"(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b);

''(2) issued a subpoena pursuant to subsection (c);

''(3) brought a civil action pursuant to subsection (c)(2); or

''(4) conducted additional actions pursuant to subsection (d).

''SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) DISCLOSURE, RETENTION, AND USE.—

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Office or Agency pursuant to section 2232 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

''(A) a cybersecurity purpose;

''(B) the purpose of identifying—

''(i) a cyber threat, including the source of the cyber threat; or

''(ii) a security vulnerability;

''(C) the purpose of responding to, or otherwise preventing or mitigating, a specific

threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

"(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

"(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a covered cyber incident or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

"(2) AGENCY ACTIONS AFTER RECEIPT.—

"(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Office shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and

rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

"(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

"(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Office pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

"(A) personal information of a specific individual; or

"(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(4) DIGITAL SECURITY.—The Office shall ensure that reports submitted to the Office pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

"(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Office in accordance with this subtitle to regulate, including through an enforcement action, the lawful activities of any non-Federal entity.

"(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report under section 2232 to the Office shall not constitute a waiver of any applicable privilege

or protection provided by law, including trade secret protection and attorney-client privilege.

''(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

''(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

''(e) LIABILITY PROTECTIONS.—

''(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rules promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

''(2) SCOPE.—The liability protections provided in subsection (c) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Office, and nothing in this subtitle shall create a defense to a discovery request, or otherwise limit or affect the discovery of information from a cause of action authorized under any Federal, State, local, or Tribal law.

''(f) SHARING WITH FEDERAL AND NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

''(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.''.

(c) 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 items relating to subtitle B of title XXII the following:

''Subtitle C—Cyber Incident Reporting

SEC. 4. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—Notwithstanding any other provision of law or regulation, any Federal agency that receives a report from an entity of a cyber attack, including a ransomware attack, shall provide all such information to the Director of the Cybersecurity Infrastructure Security Agency not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cyber Incident Review Office established under section 2231 of the Homeland Security Act of 2002, as added by section 3(b) of this Act, and another Federal entity.

(b) CREATION OF COUNCIL.—Section 1752(c)(1) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)) is amended—

(1) in subparagraph (G), by striking "and" at the end;

(2) by redesignating subparagraph (H) as subparagraph (I); and

(3) by inserting after subparagraph (G) the following:

"(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and".

(c) HARMONIZING REPORTING REQUIREMENTS.—The National Cyber Director shall, in consultation with the Director, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) review existing regulatory requirements, including the information required in such reports, to

report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 5. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) PROGRAM.—Not less than 90 days after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures, and to dedicate resources, to identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

~~(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—~~ ~~The pilot program established under subsection (a) shall—~~

~~(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and~~

~~(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).~~

~~(c) ENTITY NOTIFICATION.—~~

~~(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.~~

~~(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.~~

~~(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information~~

on the identified security vulnerability and mitigation techniques.

(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practical, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

SEC. 6. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) JOINT RANSOMWARE TASK FORCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the National Cyber Director shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing, nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) CLARIFYING PRIVATE-SECTOR LAWFUL DEFENSIVE MEASURES.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judi-

ciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private-sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as providing any additional authority to any Federal agency.

SEC. 7. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the interim final rule under section 2232(b)(1) of the Homeland Security Act of 2002, as added by section 3(b) of this Act, the Director 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 that describes how the Director engaged stakeholders in the development of the interim final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director 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 de-

scribing how the Cyber Incident Review Office has carried out activities under section 2231(b)(9) of the Homeland Security Act of 2002, as added by section 3(b) of this Act, by proactively identifying opportunities to use cyber incident data to inform and enabling cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 5, the Director 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, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 5(c) to mitigate security vulnerabilities and the threat of ransomware.

(2) The identification of most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(1) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(2) any actions the National Cyber Director intends to take to harmonize the duplicative reporting requirements; and

(3) any proposed legislative changes necessary to address the duplicative reporting.

(e) GAO REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States 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 implementation of this Act and the amendments made by this Act.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Incident Reporting Act of 2021".

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms "covered cyber incident", "covered entity", and "cyber incident" have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 3(b) of this Act.

(2) CYBER ATTACK; RANSOM PAYMENT; RANSOMWARE ATTACK.—The terms "cyber attack", "ransom payment", and "ransomware attack" have the meanings given those terms in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651), as amended by section 3(a) of this Act.

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

(4) INFORMATION SYSTEM; SECURITY VULNERABILITY.—The terms "information system" and "security vulnerability" have the meanings given those

terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

SEC. 3. CYBER INCIDENT REPORTING.

(a) DEFINITIONS.—

(1) IN GENERAL.—Section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), and (6) as paragraphs (2), (4), (5), (7), (10), and (11), respectively;

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

"(1) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.";

(C) by inserting after paragraph (2), as so redesignated, the following:

"(3) CYBER ATTACK.—The term 'cyber attack' means the use of unauthorized or malicious code on an information system, or the use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information

system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system.";

(D) by inserting after paragraph (5), as so redesignated, the following:

"(6) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.";

(E) by inserting after paragraph (7), as so redesignated, the following:

"(8) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

"(9) RANSOMWARE ATTACK.—The term 'ransomware attack'—

"(A) means a cyber attack that includes the threat of use of unauthorized or malicious code on an information system, or the threat of use of another digital mechanism such as a denial of

service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is made by a Federal Government entity, good-faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system."; and

(F) by adding at the end the following:

"(13) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber attack that allows an adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (such as information technology products), or services at any point during the life cycle.

"(14) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value

that functions as a medium of exchange, a unit of account, or a store of value.

"(15) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.".

(2) CONFORMING AMENDMENT.—Section 9002(A)(7) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(a)(7)) is amended to read as follows:

"(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651).".

(b) CYBER INCIDENT REPORTING.—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—Cyber Incident Reporting

"SEC. 2230. DEFINITIONS.

"(a) IN GENERAL.—Except as provided in subsection (b), the definitions under section 2201 shall apply to this subtitle.

"(b) ADDITIONAL DEFINITIONS.—In this subtitle:

"(1) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

"(2) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the interim final rule and final rule issued pursuant to section 2232.

"(3) COVERED ENTITY.—The term 'covered entity' means an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the interim final rule and final rule issued pursuant to section 2232.

"(4) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2209(a).

"(5) CYBER THREAT.—The term 'cyber threat'—

"(A) has the meaning given the term 'cybersecurity threat' in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501); and

"(B) does not include any activity related to good faith security research, including partici-

pation in a bug-bounty program or a vulnerability disclosure program.

"(6) CYBER THREAT INDICATOR; CYBERSECURITY PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL; SECURITY VULNERABILITY.—The terms 'cyber threat indicator', 'cybersecurity purpose', 'defensive measure', 'Federal entity', 'information system', 'security control', and 'security vulnerability' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

"(7) SMALL ORGANIZATION.—The term 'small organization'—

"(A) means—

"(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

"(ii) any business, nonprofit organization, or other private sector entity with fewer than 50 employees (determined on a full-time equivalent basis); and

"(B) does not include—

"(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

"(ii) a business, nonprofit organization, or other private sector entity that holds a government contract, unless that contractor is a party only to—

"(I) a service contract to provide housekeeping or custodial services; or

"(II) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

"SEC. 2231. CYBER INCIDENT REVIEW OFFICE.

"(a) CYBER INCIDENT REVIEW OFFICE.—There is established in the Agency a Cyber Incident Review Office (in this section referred to as the 'Office') to receive, aggregate, and analyze reports related to covered cyber incidents submitted by covered entities and reports related to ransom payments submitted by entities in furtherance of the activities specified in subsection (b) of this section and sections 2202(e), 2203, and 2209(c) and any other authorized activity of the Director to enhance the situational awareness of cyber threats across critical infrastructure sectors.

"(b) ACTIVITIES.—The Office shall, in furtherance of the activities specified in sections 2202(e), 2203, and 2209(c)—

"(1) receive, aggregate, analyze, and secure, consistent with the requirements under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls and identify tactics, techniques, and procedures adversaries use to overcome those controls;

"(2) receive, aggregate, analyze, and secure reports related to ransom payments to identify tactics, techniques, and procedures, including identifying and tracking ransom payments utilizing virtual currencies, adversaries use to perpetuate ransomware attacks and facilitate ransom payments;

"(3) leverage information gathered about cybersecurity incidents to—

"(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers; and

"(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber attack campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures;

"(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

"(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

"(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a substantial cyber incident, or is part of a group

of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

"(7) with respect to covered cyber incident reports under subsection (c) involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

"(8) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the reports required under subsection (c);

"(9) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransom attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

"(10) proactively identify opportunities, consistent with the protections in section 2235, to lever-

age and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

"(11) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Office; and

"(12) in accordance with section 2235, not later than 24 hours after receiving a covered cyber incident report or ransom payment report, share the reported information with appropriate Sector Risk Management Agencies and other appropriate agencies as determined by the Director of Office Management and Budget, in consultation with the Director and the National Cyber Director.

"(c) PERIODIC REPORTING.—Not later than 60 days after the effective date of the interim final rule required under section 2232(b)(1), and on the first day of each month thereafter, the Director, in consultation with the Attorney General and the Director of National Intelligence,

shall submit to the National Cyber Director, the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the report, which shall—

"(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

"(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

"(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

"(B) intelligence gaps that have, or currently are, impeding the ability to counter covered cyber incidents and ransomware threats;

"(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

"(4) be unclassified, but may include a classified annex.

"(d) ORGANIZATION.—The Director may organize the Office within the Agency as the Director deems appropriate, including harmonizing the functions of the Office with other authorized activities.

"SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

"(a) IN GENERAL.—

"(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

"(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual, a small organization, or a religious institution, that makes a ransom payment as the result of

a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

"(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

"(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the interim final rule and final rule issued pursuant to subsection (b).

"(5) EXCEPTIONS.—

"(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with proce-

dures established in the interim final rule and final rule issued pursuant to subsection (b).

"(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

"(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed according to the interim final rule and final rule issued pursuant to subsection (b).

"(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the interim final rule and the final rule issued pursuant to subsection (b), except that the requirements of paragraphs (1) through (4) shall not be effective for a period for more than 18 months after the effective date of the interim final rule if the Director has not issued a final rule pursuant to subsection (b)(2).

"(b) RULEMAKING.—

"(1) INTERIM FINAL RULE.—Not later than 270 days after the date of enactment of this section, and after a 60-day consultative period, followed by a 90-day comment period with appropriate stakeholders, the Director, in consultation with Sector Risk Management Agencies and the heads of other Federal agencies, shall publish in the Federal Register an interim final rule to implement subsection (a).

"(2) FINAL RULE.—Not later than 1 year after publication of the interim final rule under paragraph (1), the Director shall publish a final rule to implement subsection (a).

"(3) SUBSEQUENT RULEMAKINGS.—Any rule to implement subsection (a) issued after publication of the final rule under paragraph (2), including a rule to amend or revise the final rule issued under paragraph (2), shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

"(c) ELEMENTS.—The interim final rule and final rule issued pursuant to subsection (b) shall be composed of the following elements:

"(1) A clear description of the types of entities that constitute covered entities, based on—

"(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

"(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

"(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

"(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

"(A) at a minimum, require the occurrence of—

"(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety

and resiliency of operational systems and processes;

"(ii) a disruption of business or industrial operations due to a cyber incident; or

"(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

"(B) consider—

"(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

"(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

"(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

"(C) exclude—

"(i) any event where the cyber incident is perpetuated by a United States Government entity, good-faith security research, or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as a through a vulnerability disclosure program or the use of authorized penetration testing services; and

"(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

"(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

"(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

"(A) A description of the covered cyber incident, including—

"(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

"(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

"(iii) the estimated date range of such incident; and

"(iv) the impact to the operations of the covered entity.

"(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

"(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

"(D) Where applicable, identification of the category or categories of information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

"(E) The name and, if applicable, taxpayer identification number or other unique identifier of the entity impacted by the covered cyber incident.

"(F) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission, and at the direction, of the covered entity to assist with compliance with the requirements of this subtitle.

"(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

"(A) A description of the ransomware attack, including the estimated date range of the attack.

"(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

"(C) Where applicable, any identifying or contact information related to the actor or actors

reasonably believed to be responsible for the ransomware attack.

"(D) The name and, if applicable, taxpayer identification number or other unique identifier of the entity that made the ransom payment.

"(E) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

"(F) The date of the ransom payment.

"(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

"(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

"(I) The amount of the ransom payment.

"(J) A summary of the due diligence review required under subsection (e).

"(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

"(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

"(A) be established by the Director in consultation with the Council;

"(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

"(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

"(8) Procedures for—

"(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), which shall include, at a minimum, a concise, user-friendly web-based form;

"(B) the Office to carry out the enforcement provisions of section 2233, including with respect to the issuance of subpoenas and other aspects of noncompliance;

"(C) implementing the exceptions provided in subparagraphs (A), (B), and (D) of subsection (a)(5); and

"(D) anonymizing and safeguarding information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

"(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

"(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law

firm, to submit the required report under subsection (a).

"(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

"(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

"(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding a due diligence review under subsection (e) and reporting ransom payments under this section.

"(e) DUE DILIGENCE REVIEW.—Before the date on which a covered entity, or an entity that would be required to submit a ransom payment report under this section if that entity makes a ransom payment, makes a ransom payment relating to a ransomware attack, the covered entity

or entity shall conduct a due diligence review of alternatives to making the ransom payment, including an analysis of whether the covered entity or entity can recover from the ransomware attack through other means.

"(f) OUTREACH TO COVERED ENTITIES.—

"(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

"(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

"(A) An overview of the interim final rule and final rule issued pursuant to subsection (b).

"(B) An overview of mechanisms to submit to the Office covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

"(C) An overview of the protections afforded to covered entities for complying with the re-

quirements under paragraphs (1), (2), and (3) of subsection (a).

"(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

"(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

"(F) An overview of the privacy and civil liberties requirements in this subtitle.

"(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

"(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

"(B) information sharing and analysis organizations;

"(C) trade associations;

"(D) information sharing and analysis centers;

"(E) sector coordinating councils; and

"(F) any other entity as determined appropriate by the Director.

"(g) EVALUATION OF STANDARDS.—

"(1) IN GENERAL.—Before issuing the final rule pursuant to subsection (b)(2), the Director shall review the data collected by the Office, and in consultation with other appropriate entities, assess the effectiveness of the rule with respect to—

"(A) the number of reports received;

"(B) the utility of the reports received;

"(C) the number of supplemental reports required to be submitted; and

"(D) any other factor determined appropriate by the Director.

"(2) SUBMISSION TO CONGRESS.—The Director 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 the results of the evaluation described in paragraph (1) and may thereafter, in accordance with the requirements under subsection (b), publish in the Federal Register a final rule implementing this section.

"(h) ORGANIZATION OF REPORTS.—Notwithstanding chapter 35 of title 44, United States Code (commonly

known as the 'Paperwork Reduction Act'), the Director may reorganize and reformat the means by which covered cyber incident reports, ransom payment reports, and any other voluntarily offered information is submitted to the Office.

"SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

"(a) IN GENERAL.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

"(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

"(c) APPLICATION OF PROTECTIONS.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

"SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

"(a) PURPOSE.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may

obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

"(b) INITIAL REQUEST FOR INFORMATION.—

"(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(b), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Office within 72 hours in accordance to section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

"(2) TREATMENT.—Information provided to the Office in response to a request under paragraph (1)

shall be treated as if it was submitted through the reporting procedures established in section 2232.

"(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

"(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

"(2) CIVIL ACTION.—

"(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

"(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

"(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as a contempt of court.

"(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

"(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity with a Federal Government contract, grant, or cooperative agreement fails to comply with a subpoena issued under this subsection—

"(A) the Director may refer the matter to the Administrator of General Services; and

"(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

"(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

"(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Director determines, based on the information provided in response to the subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may con-

stitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide that information to the Attorney General or the appropriate regulator, who may use that information for a regulatory enforcement action or criminal prosecution.

"(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Office by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

"(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

"(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

"(1) the size and complexity of the entity;

"(2) the complexity in determining if a covered cyber incident has occurred;

"(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments; and

"(4) for non-covered entities required to submit a ransom payment report, the ability of the entity to perform a due diligence review pursuant to section 2232(e).

"(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

"(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

"(1) issued an initial request for information pursuant to subsection (b);

"(2) issued a subpoena pursuant to subsection (c);

"(3) brought a civil action pursuant to subsection (c)(2); or

"(4) conducted additional actions pursuant to subsection (d).

"SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

"(a) DISCLOSURE, RETENTION, AND USE.—

"(1) AUTHORIZED ACTIVITIES.—Information provided to the Office or Agency pursuant to section 2232 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

"(A) a cybersecurity purpose;

"(B) the purpose of identifying—

"(i) a cyber threat, including the source of the cyber threat; or

"(ii) a security vulnerability;

"(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

"(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

"(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a covered cyber incident or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

"(2) AGENCY ACTIONS AFTER RECEIPT.—

"(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Office shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

"(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and

manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

"(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Office pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

"(A) personal information of a specific individual; or

"(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(4) DIGITAL SECURITY.—The Office shall ensure that reports submitted to the Office pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for mod-

erate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

"(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Office in accordance with this subtitle to regulate, including through an enforcement action, the lawful activities of any non-Federal entity.

"(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report under section 2232 to the Office shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

"(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

"(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be sub-

ject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision making official.

"(e) LIABILITY PROTECTIONS.—

"(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rules promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

"(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Office.

"(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other pro-

ceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

"(f) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

"(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.".

(c) 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 items relating to subtitle B of title XXII the following:

"Subtitle C—Cyber Incident Reporting

"Sec. 2230. Definitions.
"Sec. 2231. Cyber Incident Review Office.
"Sec. 2232. Required reporting of certain cyber incidents.

SEC. 4. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—Notwithstanding any other provision of law or regulation, any Federal agency that receives a report from an entity of a cyber attack or cyber incident, including a ransomware attack, shall provide all such information to the Director of the Cybersecurity Infrastructure Security Agency not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cyber Incident Review Office established under section 2231 of the Homeland Security Act of 2002, as added by section 3(b) of this Act, and another Federal entity.

(b) CREATION OF COUNCIL.—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is amended—

(1) in paragraph (1)—

(A) in subparagraph (G), by striking "and" at the end;

(B) by redesignating subparagraph (H) as subparagraph (I); and

(C) by inserting after subparagraph (G) the following:

"(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and"; and

(2) by adding at the end the following:

"(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any Federal entity.".

(c) HARMONIZING REPORTING REQUIREMENTS.—The National Cyber Director shall, in consultation with the Director, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021

(6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 5. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) PROGRAM.—Not later than 90 days after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures, and to dedicate resources, to iden-

tifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).

(c) ENTITY NOTIFICATION.—

(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and

notify the entity at risk pursuant to the procedures within that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practical, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

SEC. 6. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) JOINT RANSOMWARE TASK FORCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing,

nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) CLARIFYING PRIVATE-SECTOR LAWFUL DEFENSIVE MEASURES.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee

on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private-sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 7. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the interim final rule under section 2232(b)(1) of the Homeland Security Act of 2002, as added by section 3(b) of this Act, the Director shall submit to the Committee on Homeland Security and Government Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the interim final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Government Affairs

of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the Cyber Incident Review Office has carried out activities under section 2231(b)(9) of the Homeland Security Act of 2002, as added by section 3(b) of this Act, by proactively identifying opportunities to use cyber incident data to inform and enabling cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 5, the Director 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, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 5(c) to mitigate security vulnerabilities and the threat of ransomware.

(2) The identification of most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the National Cyber Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) GAO REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States 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 implementation of this Act and the amendments made by this Act.

Calendar No. 633

117TH CONGRESS
2D SESSION

S. 2875

[Report No. 117–249]

A BILL

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

DECEMBER 13, 2022

Reported with an amendment