117TH CONGRESS
1ST SESSION

S. _____

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

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on _____

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. 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 (3), (4), (5), (6), (9), and (10), respectively;

(B) by inserting before paragraph (3), as so redesignated, the following:

''(1) COVERED CYBERSECURITY INCIDENT.—The term 'covered cybersecurity incident' means a cybersecurity incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the interim rule and final rule issued pursuant to section 2220A(d).

''(2) 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 rule and final rule issued pursuant to section 2220A(d).'';

(C) in paragraph (5), as so redesignated, by striking ''The term'' and inserting ''Except as otherwise provided, the term'';

(D) by inserting after paragraph (6), as so redesignated, the following:

"(7) 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.

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

"(A) 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 in connection with a demand for a ransom payment;

"(B) 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

''(C) 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 operator of the information system for third parties to find vulnerabilities in the information system.''; and

(E) by adding at the end the following:

''(11) 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.

''(12) 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) is amended—

(A) by striking ''the term 'Sector-Specific Agency' '' and inserting ''the term 'Sector Risk Management Agency' '';

(B) by striking ''section 2201(5)'' and inserting ''section 2201''; and

(C) by striking ''6 U.S.C. 651(5)'' and inserting ''6 U.S.C. 651''.

(b) CYBER INCIDENT REPORTING.—Subtitle A of 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: ***[****NOTE: The numbering below assumes that the technical and conforming amendments to title XXII that we were working on have been enacted. We can't draft with that assumption, but I'll leave them numbered as is in case those changes are enacted as we work through this draft.****]***

''SEC. 2220A. CYBER INCIDENT REVIEW OFFICE.

''(a) DEFINITIONS.—In this section:

''(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.

''(2) COUNCIL.—The term 'Council' means the Cybersecurity Incident Reporting Council described in section 2202(e)(1)(S).

"(3) 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).

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

"(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat'—

"(A) has the meaning given the term 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) 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 reg-

ular support and active administration on the premises of a customer, in the data center of the managed service provider (such as hosting) or in a third-party data center.

''(7) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(8) SMALL BUSINESS.—The term 'small business'—

''(A) means a business with less than 50 employees (determined on a full-time equivalent basis);

''(B) does not include a business that is a covered entity; and

''(C) does not include 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.

"(9) SUPPLY CHAIN ATTACK.—The term 'supply chain attack' means an 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.

"(b) 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 cybersecurity 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 cybersecurity threats across critical infrastructure sectors.

''(c) ACTIVITIES.—The Office shall, in furtherance of the activities specified in sections 2202(e), 2203, and 2209(c) and any other authorized activity of the Director—

''(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 cybersecurity 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) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cybersecurity incidents and ransom payments, particularly with respect to ongoing cybersecurity threats or security vulnerabilities;

''(4) for a covered cybersecurity incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or are part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cybersecurity incident or group of those incidents and identify ways to prevent or mitigate similar incidents in the future;

''(5) with respect to covered cybersecurity incident reports under subsection (d) involving an ongoing cybersecurity 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;

''(6) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cybersecurity incident and ransom payment reports under subsection (d);

''(7) proactively identify opportunities and perform analyses, consistent with the protections in section 2220C, 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;

''(8) proactively identify opportunities, consistent with the protections in section 2220C, to leverage and utilize data on cybersecurity 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; and

''(9) 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 Security and Exchange Commission by entities experiencing cybersecurity incidents and compare such disclosures to reports received by the Office.

''(d) COVERED CYBERSECURITY INCIDENT AND RANSOM PAYMENT REPORTING REQUIREMENTS AND PROCEDURES.—

''(1) IN GENERAL.—The Director, in consultation with Sector Risk Management Agencies and the heads of other Federal departments and agencies, as appropriate, shall—

''(A) not later than 270 days after the date of the enactment of this section, and after a 60-

day consultative period, followed by a 90-day comment period with appropriate stakeholders, publish in the Federal Register an interim final rule implementing this section that shall—

''(i) require covered entities to submit to the Office reports containing information relating to covered cybersecurity incidents;

''(ii) establish procedures that clearly describe—

''(I) the types of critical infrastructure determined to be covered entities;

''(II) the types of cybersecurity incidents determined to be covered cybersecurity incidents;

''(III) all the mechanisms by which covered cybersecurity incident reports under clause (i) are to be submitted, including—

''(aa) the contents, as described in paragraph (5), to be included in each such report, including any supplemental reporting requirements;

"(bb) the timing relating to when each such report should be submitted; and

"(cc) the format of each such report;

"(IV) the manner in which the Office will carry out the enforcement provisions of section 2220B, including with respect to the issuance of subpoenas, conducting of examinations, public reporting of entities, and other aspects of noncompliance;

"(V) an exemption to the requirement to submit to the Office a covered cybersecurity incident report in the event—

"(aa) the covered entity submits substantially the same information about the covered cybersecurity incident as would be required to be submitted to the Office to a different regulatory authority or Federal entity within the same timeframe for reporting established in this section; and

"(bb) agreements are in place to ensure the different regulatory authority or Federal entity will transmit the relevant information to the Office within 24 hours of receipt; and

"(VI) any other responsibilities to be carried by covered entities, or other procedures necessary to implement this section;

"(iii) require entities, including covered entities and except for individuals and small businesses, that make a ransom payment, either directly or through a third party, as the result of a ransomware attack against the entity to submit to the Office reports containing information relating to the ransomware attack and ransom payment;

"(iv) not require covered entities to submit separate reports for a covered incident and a ransom payment if a ransom payment is made in response to a covered incident, except if a covered entity makes a covered incident report prior to making

a ransom payment and subsequently makes a ransom payment, the interim final rule shall require a supplemental report including the ransom payment information be submitted pursuant to paragraph (5)(E);

''(v) require the anonymization and safeguarding of information received and disclosed through covered incident reports and ransom payment reports that may be used to identify specific persons unrelated to a covered incident or ransom payment; and

''(vi) notwithstanding section 553 of title 5, United States Code, be effective, on an interim basis, immediately upon publication, but may be subject to change and revision after public notice and opportunity for comment; and

''(B) issue a final rule not later than 1 year after publication of the interim final rule under subparagraph (A).

''(2) CONSIDERATIONS FOR COVERED ENTITIES.—In determining which types of critical infrastructure are covered entities for purposes of this section, the Director, in consultation with Sector

Risk Management Agencies and the heads of other Federal departments and agencies, as appropriate, shall consider—

"(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.

"(3) COVERED CYBERSECURITY INCIDENTS.—

"(A) CONSIDERATIONS AND EXCLUSIONS.—In determining which types of incidents are covered cybersecurity incidents for purposes of this section, the Secretary shall—

"(i) 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

''(ii) exclude—

''(I) any event where the cybersecurity incident is perpetuated by a United States Government entity, good-faith security research, or in response to an invitation by the 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; or

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

"(B) MINIMUM THRESHOLDS.—In order for a cybersecurity incident to be considered a covered cybersecurity incident for purposes of this section, a cybersecurity incident shall, at a minimum, involve not less than 1 of the following:

"(i) Unauthorized access to an information system or network has occurred and lead to loss of confidentiality, integrity, or availability of such information system or network, or has a serious impact on the safety and resiliency of operational systems and processes.

"(ii) Disruption of business or industrial operations has occurred due to a cybersecurity incident, such as due to a distributed denial of service attack, a ransomware attack, or exploitation of a zero-day vulnerability against an information system, operational technology system or process, or network.

"(iii) Unauthorized access or disruption of business operations has occurred due to loss of service facilitated through, or caused by—

"(I) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

"(II) a supply chain attack.

"(4) OUTREACH TO COVERED ENTITIES.—

"(A) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform covered entities, entities that make a ransom payment, and entities that make ransom payments on behalf of entities impacted by ransomware attacks of the requirements of this section.

"(B) ELEMENTS.—The outreach and education campaign under subparagraph (A) shall include the following:

"(i) An overview of the interim final rule and final rule issued pursuant to this section.

"(ii) An overview of mechanisms to submit to the Office covered cybersecurity

incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

"(iii) An overview of the protections afforded to covered entities for complying with the requirements under subsection (f).

"(iv) An overview of the steps taken under section 2220B when a covered entity is not in compliance with the reporting requirements under paragraph (1).

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

"(C) COORDINATION.—In conducting the outreach and education campaign required under subparagraph (A), the Director may coordinate with—

"(i) the Critical Infrastructure Partnership Advisory Council established under section 871 (6 U.S.C. 451);

"(ii) information sharing and analysis organizations; and

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

"(5) REPORTS.—

"(A) TIMING.—The Director, in consultation with Sector Risk Management Agencies and the heads of other Federal departments and agencies, as appropriate, shall establish reporting timelines for covered entities to submit covered cybersecurity incident and ransom payment reports to the Office promptly, as the Director determines reasonable and appropriate based on relevant factors, such as the nature of the incident and the time required for investigation, but in no case may the Director require reporting—

"(i) for covered incidents, earlier than 72 hours or later than 7 days after it is reasonably believed that a covered cybersecurity incident has occurred; and

"(ii) for ransom payments, earlier than 24 hours or later than 72 hours after a ransom payment has been made.

"(B) CONSIDERATIONS.—In establishing reporting deadlines, the Director shall—

"(i) consult with the Council;

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

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

"(C) SUPPLEMENTAL REPORTING.—A covered entity shall submit promptly to the Office an update or supplement to a previously submitted covered cybersecurity incident report if new or different information becomes available, or if the covered entity makes a ransomware payment after submitting a report prior to making a payment, that would otherwise have been required to have been included in such previously submitted report.

"(D) COVERED INCIDENT REPORT CONTENTS.—Covered cybersecurity incident reports

submitted pursuant to this section shall contain such information as the Director prescribes, including the following information, to the extent applicable and available, with respect to a covered cybersecurity incident:

''(i) A description of the covered cybersecurity incident, including identification of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident, and the estimated date range of such incident.

''(ii) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cybersecurity incident.

''(iii) Where applicable, any identifying or contact information related to the actor responsible for such incident.

''(iv) 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.

"(v) The name and, where applicable, the taxpayer identification number, or other unique identifier of the entity impacted by the covered cybersecurity incident.

"(vi) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the covered entity or agent of such covered entity, or, where applicable, the service provider of such covered entity.

"(E) RANSOM PAYMENT REPORT CONTENTS.—Ransom payment reports submitted pursuant to this section shall contain such information as the Director prescribes, including the following information, to the extent applicable and available, with respect to a ransom payment:

"(i) A description of the ransomware attack that led to the ransom payment, including the estimated date range of the ransomware attack.

"(ii) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the

ransomware attack that led to the ransom payment.

''(iii) Where applicable, any identifying or contact information related to the actor responsible for the ransomware attack that led to the ransom payment.

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

''(v) Contact information, such as a telephone number or electronic mail address, that the Office may use to contact the entity that made the ransom payment or the agent of that entity, or, where applicable, the service provider of that entity.

''(vi) The date of the ransom payment.

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

''(viii) The ransom payment instructions, including information relating to where to send the ransom payment, such as the virtual currency address or the

physical address the funds were requested to be sent to, if applicable.

''(ix) The amount of the ransom payment.

''(x) A summary of the due diligence review required under subparagraph (F).

''(F) 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—

''(i) a search for potential decryption methods; and

''(ii) an analysis of whether the covered entity or entity can recover from the ransomware attack through other means.

''(G) HARMONIZING REPORTING REQUIREMENTS.—In establishing the reporting requirements and procedures under paragraph (1), the Director shall, in consultation with the Council to the maximum extent practicable—

"(i) review existing regulatory requirements, including the information required in such reports, to report cybersecurity incidents that may apply to covered entities, and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

"(ii) coordinate with other regulatory authorities that receive reports relating to cybersecurity incidents to identify opportunities to streamline reporting processes, and where feasible, enter into agreements with such authorities to permit the sharing of such reports with the Office, consistent with applicable law and policy, without impacting the Office's ability to gain timely situational awareness of a covered cybersecurity incident or significant cyber incident.

"(H) FLEXIBLE REPORTING.—In prescribing reporting deadlines for a report required under this paragraph, the Director may choose to establish a flexible, phased reporting timeline for covered entities to report informa-

tion about cybersecurity incidents in a manner that aligns with investigative timelines and allows entities to prioritize incident response efforts over compliance.

''(6) EVALUATION OF STANDARDS.—Not more than 1 year after the issuance of the interim final rule pursuant to paragraph (1), the Director shall review the data collected by the Office, and in consultation with other appropriate Federal agencies and non-Federal 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.

''(7) 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 (6) and may, as appropriate, after a 60 day consultative period, followed by a 90-day comment period with appropriate stakeholders,

publish in the Federal Register an interim final rule to update the implementation of this section.

''(e) VOLUNTARY REPORTING OF CYBER INCIDENTS.—

''(1) IN GENERAL.—The Agency shall receive cybersecurity incident reports and ransom payment reports submitted voluntarily by entities that are not covered entities, or concerning cybersecurity incidents that do not satisfy the definition of covered cybersecurity incidents, or concerning ransomware attacks where no ransom payment is made, but may enhance the situational awareness of the Agency of cybersecurity threats.

''(2) APPLICATION OF PROTECTIONS.—The protections under section 2220C applicable to covered cybersecurity incident reports shall apply in the same manner and to the same extent to voluntarily-submitted cybersecurity incident reports under this subsection.

''(3) ADDITIONAL VOLUNTARY INFORMATION IN MANDATORY REPORTS.—The Agency shall receive cybersecurity incident reports and ransom payment reports that are required to be submitted by covered entities and entities that make ransom payments with any additional, voluntarily included, informa-

tion that the submitting entity chooses to include to enhance the situational awareness of the Agency of cybersecurity threats.

''(f) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

''(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered 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 (b).

''(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 (d)(1)(A)(iii).

''(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 incident report or ransom payment report submission.

''(4) RESPONSIBILITY TO ADVISE.—Any third party that makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the impacted entities responsibilities regarding a due diligence review under subsection (d)(5)(F) and reporting of ransom payments under this section.

''SEC. 2220B. NONCOMPLIANCE WITH REQUIRED REPORTING.

''(a) PURPOSE.—In the event that an entity that is required to submit a report in section 2220A 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, or, if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, subject to the limitations of subsection (c), to gather information sufficient to determine whether a covered cybersecurity 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, intelligence gathering, or other information in the posses-

sion of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2220A(c), that an entity has experienced a covered cybersecurity incident or made a ransomware payment but failed to report such incident or payment to the Office in accordance to section 2220A(d), the Director shall request additional information from the entity to confirm whether or not a covered cybersecurity incident or ransomware payment has occurred, and determine whether further examination into the details surrounding the incident or payment are warranted pursuant to subsection (d).

''(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 2220A.

''(c) AUTHORITY TO ISSUE SUBPOENAS.—

''(1) IN GENERAL.—If, after the date that is 7 days 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 infor-

mation the Director deems necessary to determine whether a covered cybersecurity incident or ransomware payment has occurred and assess potential impacts to national security, economic security, public health and safety, determine whether further examination into the details surrounding such incident are warranted pursuant to subsection (d), and, if so, compel disclosure of that information as is necessary to carry out activities under section 2220A(c).

''(2) CIVIL ACTION.—

''(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may 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.

''(d) ADDITIONAL ACTIONS.—

"(1) EXAMINATION.—If, based on the information provided in response to a subpoena issued pursuant to subsection (c), the Director determines that the incident is a significant cyber incident, or is part of a group of related cyber incidents that together meet the definition, or if the entity did not report a ransomware payment, and a more thorough examination of the details surrounding such incident is warranted in order to carry out activities under section 2220A, the Director may direct the Office to conduct an examination of the incident in order to enhance the situational awareness of the Agency of cybersecurity threats (as defined in section 2220A) across critical infrastructure sectors and payments made to ransomware actors, in a manner consistent with privacy and civil liberties under section 2220C(b)(3).

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

"(A) IN GENERAL.—Notwithstanding section 2220C(b) 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) or identified in the course of an examination under

paragraph (1), that the facts relating to the covered cybersecurity 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.

"(B) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered incident or ransom payment report submitted to the Office by an entity that makes a ransom payment or third party under section 2220A shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity or third party.

"(C) NO IMMUNITY.—An entity that submits a covered incident or ransom payment report under section 2220A is not granted any immunity from law enforcement action for making a ransom payment.

''(e) CONSIDERATIONS.—When determining whether to impose a penalty on an entity, the Director shall take into consideration—

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

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

''(3) prior interaction with the Agency or awareness of the entity of Agency policies and procedures for reporting covered 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 2220A(d)(5)(F).

''(f) EXCLUSIONS.—The penalties for failure to submit a covered incident report or a ransom payment report shall not apply to a State, local, Tribal, or territorial government entity.

''SEC. 2220C. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) CYBERSECURITY THREAT DEFINED.—In this section, the term 'cybersecurity threat' has the meaning given the term in section 2220A.

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

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Office or Agency in accordance with section 2220A 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 cybersecurity threat, including the source of the cybersecurity 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 cybersecurity 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) EXCEPTIONS.—

''(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cybersecurity incident 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 cybersecurity 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 cybersecurity incident 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 cybersecurity incident reports submitted to the Office pursuant to section 2220A(d) shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in a manner consistent with processes 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; and

''(4) DIGITAL SECURITY.—The Office shall ensure that reports submitted to the Office pursuant to section 2220A(d) and any related information is collected, stored, and protected in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

''(c) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Agency under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

''(d) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Agency under this Act 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.

''(e) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2220A 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.

''(f) SHARING WITH FEDERAL AND NON-FEDERAL ENTITIES.—The Agency shall facilitate the timely sharing between relevant critical infrastructure owners and operators and appropriate Federal agencies of information and analysis relating to reports received under section 2220A, particularly with respect to an ongoing cybersecurity threat or security vulnerability and anonymize the victim who reported the information.

''(g) LIABILITY PROTECTION.—The submission of a covered cybersecurity incident report or ransom payment report, including any voluntary information or reports, to the Agency under section 2220A shall be entitled to the protections against liability described in section 106 of the Cybersecurity Act of 2015 (6 U.S.C. 1505).

''(h) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2220A 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 section 2220 the following:

''Sec. 2220A. Cyber Incident Review Office.
''Sec. 2220B. Noncompliance with required reporting.
''Sec. 2220C. Information shared with or provided to the Federal Government.''.

SEC. 3. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBERSECURITY INCIDENT REPORTING SHARING.—Any Federal agency that requires an entity, either through regulation or law, to notify the Federal agency of a cyber attack, including a ransomware attack, shall provide all such information to the Director not later than 7 days after receiving the notification.

(b) CREATION OF COUNCIL.—Section 2202(e)(1) of the Homeland Security Act (6 U.S.C. 652) is amended by adding at the end the following:

"(S) To lead an intergovernmental Cybersecurity Incident Reporting Council, in coordination with the Director of the Office of Management and Budget and the National Cyber Director and in consultation with Sector Risk Management Agencies and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements (including those issued through regulations) for covered entities and entities that make a ransom payment.".

SEC. 4. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) DEFINITIONS.—In this section:

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

(2) RANSOMWARE ATTACK.—The term "ransomware attack" has the meaning given the

term in section 2201 of the Homeland Security Act of 2002, as amended by section 2(a).

(b) PILOT.—Not less than 90 days after enactment of this Act, the Director of the Cybersecurity and Information Sharing Agency (in this section referred to as the ''Director'') shall establish a ransomware vulnerability warning pilot 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.

(c) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program shall—

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

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

(d) 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 (c), 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 (c), 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 pursuant to the procedures within that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) or (2) shall include information on the identified security vulnerability and mitigation techniques.

(e) PRIORITIZATION OF NOTIFICATIONS.—To the extent practical, the Director shall prioritize covered entities, as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651), as amended by section 2(a) of this Act, for identification and notification activities.

(f) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of this pilot 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 (d).

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

SEC. 5. 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 Secretary of Homeland Security shall establish and the Joint Ransomware Task Force to coordinate an ongoing, nationwide campaign against ransomware attacks (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651), as amended by this Act), 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 Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordi-

nate 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 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 Secretary of Homeland Security, in coordination with the National Cyber Director and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on the Judiciary 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. 6. CONGRESSIONAL REPORTING.

(a) DEFINITIONS.—In this section:

(1) COVERED CYBERSECURITY INCIDENT; COVERED ENTITY; RANSOMWARE ATTACK; RANSOM PAYMENT.—the terms ''covered cybersecurity incident'', ''covered entity'', ''ransomware attack'', and ''ransom payment'' have the meaning given those terms in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651), as amended by section 2(a) this Act.

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

(b) CONGRESSIONAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Cyber Incident Review Office established under section 2220A of the Homeland Security Act of 2002, as added by this Act, 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 covered cybersecurity incidents and ransomware attacks, which shall—

(1) include the total number of reports submitted under such section 2220A during the preceding year, including a breakdown of required and voluntary reports;

(2) include any identified trends in covered cybersecurity incidents and ransomware attacks over the course of the preceding year and as compared to previous years, including any trends related to the information collected in the reports submitted under such section 2220A, 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 cybersecurity incidents and ransomware threats;

(3) include a summary of the Federal Government uses of the information in reports submitted under such section 2220A; and

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

(c) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the interim final rule required under section

2220A(d)(1) of the Homeland Security Act of 2002, as added by 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.

(d) 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 2220A(c)(7) of the Homeland Security Act of 2002, as added by this Act, by proactively identifying opportunities to use cybersecurity incident data to inform and enabling cybersecurity research within the academic and private sector.

(e) REPORT ON PILOT PROGRAM.—The Director shall annually 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 but with the presumption of declassification, on the effec-

tiveness of the pilot program established under section 4, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 4(d) 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.

(f) REPORT ON SUBPOENAS.—The Director shall annually report to Congress on—

(1) the amount of times the Director—

(A) issued an initial request for information pursuant to section 2220B(b) of the Homeland Security Act of 2002, as added by this Act;

(B) issued a subpoena pursuant to such section 2220B(c);

(C) brought a civil action pursuant to such section 2220B(c)(2); and

(D) conducted additional actions pursuant to such section 2220B(d); and

(2) explanation for any waiver or delay of publication of the names of entities that failed to submit covered incident or ransom payment reports as allowed under such section 2220B(d)(3)(A).

(g) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—Not later than 180 days after the date on which the Director convenes the Council required under subparagraph (S) of section 2202(e)(1) of the Homeland Security Act of 2002 (6 U.S.C. 652(e)(1)), as added by section 3(b), the Director shall submit to the appropriate congressional committees a report that includes—

(1) a list of duplicative Federal cybersecurity 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.

(h) 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.