

117TH CONGRESS
1ST SESSION

S. 2875

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 and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber Incident Report-
5 ing Act of 2021”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) COVERED CYBER INCIDENT; COVERED ENTI-
2 TY; CYBER INCIDENT.—The terms “covered cyber
3 incident”, “covered entity”, and “cyber incident”
4 have the meanings given those terms in section 2230
5 of the Homeland Security Act of 2002, as added by
6 section 3(b) of this Act.

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

13 (3) DIRECTOR.—The term “Director” means
14 the Director of the Cybersecurity and Infrastructure
15 Security Agency.

16 (4) INFORMATION SYSTEM; SECURITY VULNER-
17 ABILITY.—The terms “information system” and “se-
18 curity vulnerability” have the meanings given those
19 terms in section 102 of the Cybersecurity Act of
20 2015 (6 U.S.C. 1501).

21 **SEC. 3. CYBER INCIDENT REPORTING.**

22 (a) DEFINITIONS.—

23 (1) IN GENERAL.—Section 2201 of the Home-
24 land Security Act of 2002 (6 U.S.C. 651) is amend-
25 ed—

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

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

6 “(1) CLOUD SERVICE PROVIDER.—The term
7 ‘cloud service provider’ means an entity offering
8 products or services related to cloud computing, as
9 defined by the National Institutes of Standards and
10 Technology in NIST Special Publication 800–145
11 and any amendatory or superseding document relat-
12 ing thereto.”;

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

15 “(3) CYBER ATTACK.—The term ‘cyber attack’
16 means the use of unauthorized or malicious code on
17 an information system, or the use of another digital
18 mechanism such as a denial of service attack, to in-
19 terrupt or disrupt the operations of an information
20 system or compromise the confidentiality, avail-
21 ability, or integrity of electronic data stored on,
22 processed by, or transiting an information system.”;

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

1 “(6) MANAGED SERVICE PROVIDER.—The term
2 ‘managed service provider’ means an entity that de-
3 livers services, such as network, application, infra-
4 structure, or security services, via ongoing and reg-
5 ular support and active administration on the prem-
6 ises of a customer, in the data center of the entity
7 (such as hosting), or in a third-party data center.”;

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

10 “(8) RANSOM PAYMENT.—The term ‘ransom
11 payment’ means the transmission of any money or
12 other property or asset, including virtual currency,
13 or any portion thereof, which has at any time been
14 delivered as ransom in connection with a ransom-
15 ware attack.

16 “(9) RANSOMWARE ATTACK.—The term ‘ran-
17 somware attack’—

18 “(A) means a cyber attack that includes
19 the threat of use of unauthorized or malicious
20 code on an information system, or the threat of
21 use of another digital mechanism such as a de-
22 nial of service attack, to interrupt or disrupt
23 the operations of an information system or com-
24 promise the confidentiality, availability, or in-
25 tegrity of electronic data stored on, processed

1 by, or transiting an information system to ex-
2 tort a demand for a ransom payment; and

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

10 (F) by adding at the end the following:

11 “(13) SUPPLY CHAIN COMPROMISE.—The term
12 ‘supply chain compromise’ means a cyber attack that
13 allows an adversary to utilize implants or other
14 vulnerabilities inserted prior to installation in order
15 to infiltrate data, or manipulate information tech-
16 nology hardware, software, operating systems, pe-
17 ripherals (such as information technology products),
18 or services at any point during the life cycle.

19 “(14) VIRTUAL CURRENCY.—The term ‘virtual
20 currency’ means the digital representation of value
21 that functions as a medium of exchange, a unit of
22 account, or a store of value.

23 “(15) VIRTUAL CURRENCY ADDRESS.—The
24 term ‘virtual currency address’ means a unique pub-

1 lic cryptographic key identifying the location to
2 which a virtual currency payment can be made.”.

3 (2) CONFORMING AMENDMENT.—Section
4 9002(A)(7) of the William M. (Mac) Thornberry Na-
5 tional Defense Authorization Act for Fiscal Year
6 2021 (6 U.S.C. 652a(a)(7)) is amended to read as
7 follows:

8 “(7) SECTOR RISK MANAGEMENT AGENCY.—
9 The term ‘Sector Risk Management Agency’ has the
10 meaning given the term in section 2201 of the
11 Homeland Security Act of 2002 (6 U.S.C. 651).”.

12 (b) CYBER INCIDENT REPORTING.—Title XXII of
13 the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
14 is amended by adding at the end the following:

15 **“Subtitle C—Cyber Incident**
16 **Reporting**

17 **“SEC. 2230. DEFINITIONS.**

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

21 “(b) ADDITIONAL DEFINITIONS.—In this subtitle:

22 “(1) COUNCIL.—The term ‘Council’ means the
23 Cyber Incident Reporting Council described in sec-
24 tion 1752(c)(1)(H) of the William M. (Mac) Thorn-

1 berry National Defense Authorization Act for Fiscal
2 Year 2021 (6 U.S.C. 1500(c)(1)(H)).

3 “(2) COVERED CYBER INCIDENT.—The term
4 ‘covered cyber incident’ means a substantial cyber
5 incident experienced by a covered entity that satis-
6 fies the definition and criteria established by the Di-
7 rector in the interim final rule and final rule issued
8 pursuant to section 2232.

9 “(3) COVERED ENTITY.—The term ‘covered en-
10 tity’ means an entity that owns or operates critical
11 infrastructure that satisfies the definition estab-
12 lished by the Director in the interim final rule and
13 final rule issued pursuant to section 2232.

14 “(4) CYBER INCIDENT.—The term ‘cyber inci-
15 dent’ has the meaning given the term ‘incident’ in
16 section 2209(a).

17 “(5) CYBER THREAT.—The term ‘cyber
18 threat’—

19 “(A) has the meaning given the term ‘cy-
20 bersecurity threat’ in section 102 of the Cyber-
21 security Act of 2015 (6 U.S.C. 1501); and

22 “(B) does not include any activity related
23 to good faith security research, including par-
24 ticipation in a bug-bounty program or a vulner-
25 ability disclosure program.

1 “(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).

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

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

15 “(B) does not include—

16 “(i) a business that is a covered entity; or

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

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

23 “(II) a contract to provide products or services unrelated to information technology that is below the

1 micro-purchase threshold, as defined
2 in section 2.101 of title 48, Code of
3 Federal Regulations, or any successor
4 regulation.

5 **“SEC. 2231. CYBER INCIDENT REVIEW OFFICE.**

6 “(a) CYBER INCIDENT REVIEW OFFICE.—There is
7 established in the Agency a Cyber Incident Review Office
8 (in this section referred to as the ‘Office’) to receive, ag-
9 gregate, and analyze reports related to covered cyber inci-
10 dents submitted by covered entities in furtherance of the
11 activities specified in subsection (c) of this section and sec-
12 tions 2202(e), 2203, and 2209(c) and any other author-
13 ized activity of the Director to enhance the situational
14 awareness of cyber threats across critical infrastructure
15 sectors.

16 “(b) ACTIVITIES.—The Office shall, in furtherance of
17 the activities specified in sections 2202(e), 2203, and
18 2209(c)—

19 “(1) receive, aggregate, analyze, and secure,
20 consistent with the requirements under the Cyberse-
21 curity Information Sharing Act of 2015 (6 U.S.C.
22 1501 et seq.) reports from covered entities related to
23 a covered cyber incident to assess the effectiveness
24 of security controls and identify tactics, techniques,

1 and procedures adversaries use to overcome those
2 controls;

3 “(2) receive, aggregate, analyze, and secure re-
4 ports related to ransom payments to identify tactics,
5 techniques, and procedures, including identifying
6 and tracking ransom payments utilizing virtual cur-
7 rencies, adversaries use to perpetuate ransomware
8 attacks and facilitate ransom payments;

9 “(3) leverage information gathered about cyber-
10 security incidents to—

11 “(A) enhance the quality and effectiveness
12 of information sharing and coordination efforts
13 with appropriate entities, including agencies,
14 sector coordinating councils, information shar-
15 ing and analysis organizations, technology pro-
16 viders, cybersecurity and incident response
17 firms, and security researchers; and

18 “(B) provide appropriate entities, including
19 agencies, sector coordinating councils, informa-
20 tion sharing and analysis organizations, tech-
21 nology providers, cybersecurity and incident re-
22 sponse firms, and security researchers, with
23 timely, actionable, and anonymized reports of
24 cyber attack campaigns and trends, including,
25 to the maximum extent practicable, related con-

1 textual information, cyber threat indicators, and
2 defensive measures;

3 “(4) establish mechanisms to receive feedback
4 from stakeholders on how the Agency can most ef-
5 fectively receive covered cyber incident reports, ran-
6 som payment reports, and other voluntarily provided
7 information;

8 “(5) facilitate the timely sharing, on a vol-
9 untary basis, between relevant critical infrastructure
10 owners and operators of information relating to cov-
11 ered cyber incidents and ransom payments, particu-
12 larly with respect to ongoing cyber threats or secu-
13 rity vulnerabilities and identify and disseminate
14 ways to prevent or mitigate similar incidents in the
15 future;

16 “(6) for a covered cyber incident, including a
17 ransomware attack, that also satisfies the definition
18 of a substantial cyber incident, or is part of a group
19 of related cyber incidents that together satisfy such
20 definition, conduct a review of the details sur-
21 rounding the covered cyber incident or group of
22 those incidents and identify and disseminate ways to
23 prevent or mitigate similar incidents in the future;

24 “(7) with respect to covered cyber incident re-
25 ports under subsection (c) involving an ongoing

1 cyber threat or security vulnerability, immediately
2 review those reports for cyber threat indicators that
3 can be anonymized and disseminated, with defensive
4 measures, to appropriate stakeholders, in coordina-
5 tion with other divisions within the Agency, as ap-
6 propriate;

7 “(8) publish quarterly unclassified, public re-
8 ports that may be based on the unclassified informa-
9 tion contained in the reports required under sub-
10 section (c);

11 “(9) proactively identify opportunities and per-
12 form analyses, consistent with the protections in sec-
13 tion 2235, to leverage and utilize data on ransom at-
14 tacks to support law enforcement operations to iden-
15 tify, track, and seize ransom payments utilizing vir-
16 tual currencies, to the greatest extent practicable;

17 “(10) proactively identify opportunities, con-
18 sistent with the protections in section 2235, to lever-
19 age and utilize data on cyber incidents in a manner
20 that enables and strengthens cybersecurity research
21 carried out by academic institutions and other pri-
22 vate sector organizations, to the greatest extent
23 practicable;

24 “(11) on a not less frequently than annual
25 basis, analyze public disclosures made pursuant to

1 parts 229 and 249 of title 17, Code of Federal Reg-
2 ulations, or any subsequent document submitted to
3 the Securities and Exchange Commission by entities
4 experiencing cyber incidents and compare such dis-
5 closures to reports received by the Office; and

6 “(12) in accordance with section 2235, not later
7 than 24 hours after receiving a covered cyber inci-
8 dent report or ransom payment report, share the re-
9 ported information with appropriate Sector Risk
10 Management Agencies and other appropriate agen-
11 cies as determined by the Director of Office Manage-
12 ment and Budget, in consultation with the Director
13 and the National Cyber Director.

14 “(c) PERIODIC REPORTING.—Not later than 60 days
15 after the effective date of the interim final rule required
16 under section 2232(b)(1), and on the first day of each
17 month thereafter, the Director, in consultation with the
18 Attorney General and the Director of National Intel-
19 ligence, shall submit to the National Cyber Director, the
20 majority leader of the Senate, the minority leader of the
21 Senate, the Speaker of the House of Representatives, the
22 minority leader of the House of Representatives, the Com-
23 mittee on Homeland Security and Governmental Affairs
24 of the Senate, and the Committee on Homeland Security
25 of the House of Representatives a report that character-

1 izes the cyber threat facing Federal agencies and covered
2 entities, including applicable intelligence and law enforce-
3 ment information, covered cyber incidents, and ransom-
4 ware attacks, as of the date of the report, which shall—

5 “(1) include the total number of reports sub-
6 mitted under sections 2232 and 2233 during the
7 preceding month, including a breakdown of required
8 and voluntary reports;

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

15 “(A) the infrastructure, tactics, and tech-
16 niques malicious cyber actors commonly use;
17 and

18 “(B) intelligence gaps that have, or cur-
19 rently are, impeding the ability to counter cov-
20 ered cyber incidents and ransomware threats;

21 “(3) include a summary of the known uses of
22 the information in reports submitted under sections
23 2232 and 2233; and

24 “(4) be unclassified, but may include a classi-
25 fied annex.

1 “(d) ORGANIZATION.—The Director may organize
2 the Office within the Agency as the Director deems appro-
3 priate, including harmonizing the functions of the Office
4 with other authorized activities.

5 **“SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER IN-**
6 **CIDENTS.**

7 “(a) IN GENERAL.—

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

13 “(2) RANSOM PAYMENT REPORTS.—An entity,
14 including a covered entity and except for an indi-
15 vidual or a small business, that makes a ransom
16 payment as the result of a ransomware attack
17 against the entity shall report the payment to the
18 Director not later than 24 hours after the ransom
19 payment has been made.

20 “(3) SUPPLEMENTAL REPORTS.—A covered en-
21 tity shall promptly submit to the Director an update
22 or supplement to a previously submitted covered
23 cyber incident report if new or different information
24 becomes available or if the covered entity makes a

1 ransom payment after submitting a covered cyber in-
2 cident report required under paragraph (1).

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

9 “(5) EXCEPTIONS.—

10 “(A) REPORTING OF COVERED CYBER IN-
11 CIDENT WITH RANSOM PAYMENT.—If a covered
12 cyber incident includes a ransom payment such
13 that the reporting requirements under para-
14 graphs (1) and (2) apply, the covered entity
15 may submit a single report to satisfy the re-
16 quirements of both paragraphs in accordance
17 with procedures established in the interim final
18 rule and final rule issued pursuant to sub-
19 section (b).

20 “(B) SUBSTANTIALLY SIMILAR REPORTED
21 INFORMATION.—The requirements under para-
22 graphs (1), (2), and (3) shall not apply to an
23 entity required by law, regulation, or contract
24 to report substantially similar information to

1 another Federal agency within a substantially
2 similar timeframe.

3 “(6) MANNER, TIMING, AND FORM OF RE-
4 PORTS.—Reports made under paragraphs (1), (2),
5 and (3) shall be made in the manner and form, and
6 within the time period in the case of reports made
7 under paragraph (3), prescribed according to the in-
8 terim final rule and final rule issued pursuant to
9 subsection (b).

10 “(7) EFFECTIVE DATE.—Paragraphs (1)
11 through (4) shall take effect on the dates prescribed
12 in the interim final rule and the final rule issued
13 pursuant to subsection (b), except that the require-
14 ments of paragraph (1) through (4) shall not be ef-
15 fective for a period for more than 18 months after
16 the effective date of the interim final rule if the Di-
17 rector has not issued a final rule pursuant to sub-
18 section (b)(2).

19 “(b) RULEMAKING.—

20 “(1) INTERIM FINAL RULE.—Not later than
21 270 days after the date of enactment of this section,
22 and after a 60-day consultative period, followed by
23 a 90-day comment period with appropriate stake-
24 holders, the Director, in consultation with Sector
25 Risk Management Agencies and the heads of other

1 Federal agencies, shall publish in the Federal Reg-
2 ister an interim final rule to implement subsection
3 (a).

4 “(2) FINAL RULE.—Not later than 1 year after
5 publication of the interim final rule under paragraph
6 (1), the Director shall publish a final rule to imple-
7 ment subsection (a).

8 “(3) SUBSEQUENT RULEMAKINGS.—Any rule to
9 implement subsection (a) issued after publication of
10 the final rule under paragraph (2), including a rule
11 to amend or revise the final rule issued under para-
12 graph (2), shall comply with the requirements under
13 chapter 5 of title 5, United States Code, including
14 the issuance of a notice of proposed rulemaking
15 under section 553 of such title.

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

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

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

1 “(B) the likelihood that such an entity
2 may be targeted by a malicious cyber actor, in-
3 cluding a foreign country; and

4 “(C) the extent to which damage, disrup-
5 tion, or unauthorized access to such an entity,
6 including the accessing of sensitive cybersecu-
7 rity vulnerability information or penetration
8 testing tools or techniques, will likely enable the
9 disruption of the reliable operation of critical
10 infrastructure.

11 “(2) A clear description of the types of substan-
12 tial cyber incidents that constitute covered cyber in-
13 cidents, which shall—

14 “(A) at a minimum, require the occurrence
15 of—

16 “(i) the unauthorized access to an in-
17 formation system or network with a sub-
18 stantial loss of confidentiality, integrity, or
19 availability of such information system or
20 network, or a serious impact on the safety
21 and resiliency of operational systems and
22 processes;

23 “(ii) a disruption of business or indus-
24 trial operations due to a cyber incident; or

1 “(iii) an occurrence described in
2 clause (i) or (ii) due to loss of service fa-
3 cilitated through, or caused by, a com-
4 promise of a cloud service provider, man-
5 aged service provider, or other third-party
6 data hosting provider or by a supply chain
7 compromise;

8 “(B) consider—

9 “(i) the sophistication or novelty of
10 the tactics used to perpetrate such an inci-
11 dent, as well as the type, volume, and sen-
12 sitivity of the data at issue;

13 “(ii) the number of individuals di-
14 rectly or indirectly affected or potentially
15 affected by such an incident; and

16 “(iii) potential impacts on industrial
17 control systems, such as supervisory con-
18 trol and data acquisition systems, distrib-
19 uted control systems, and programmable
20 logic controllers; and

21 “(C) exclude—

22 “(i) any event where the cyber inci-
23 dent is perpetuated by a United States
24 Government entity, good-faith security re-
25 search, or in response to an invitation by

1 the owner or operator of the information
2 system for third parties to find vulnerabili-
3 ties in the information system, such as
4 through a vulnerability disclosure program
5 or the use of authorized penetration test-
6 ing services; and

7 “(ii) the threat of disruption as extor-
8 tion, as described in section 2201(8)(B).

9 “(3) A requirement that, if a covered cyber inci-
10 dent or a ransom payment occurs following an ex-
11 empted threat described in paragraph (2)(C)(ii), the
12 entity shall comply with the requirements in this
13 subtitle in reporting the covered cyber incident or
14 ransom payment.

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

20 “(A) A description of the covered cyber in-
21 cident, including—

22 “(i) identification and a description of
23 the function of the affected information
24 systems, networks, or devices that were, or

1 are reasonably believed to have been, af-
2 fected by such incident;

3 “(ii) a description of the unauthorized
4 access with substantial loss of confiden-
5 tiality, integrity, or availability of the af-
6 fected information system or network or
7 disruption of business or industrial oper-
8 ations;

9 “(iii) the estimated date range of such
10 incident; and

11 “(iv) the impact to the operations of
12 the covered entity.

13 “(B) Where applicable, a description of the
14 vulnerabilities, tactics, techniques, and proce-
15 dures used to perpetuate the covered cyber inci-
16 dent.

17 “(C) Where applicable, any identifying or
18 contact information related to each actor rea-
19 sonably believed to be responsible for such inci-
20 dent.

21 “(D) Where applicable, identification of
22 the category or categories of information that
23 was, or is reasonably believed to have been,
24 accessed or acquired by an unauthorized per-
25 son.

1 “(E) The name and, if applicable, taxpayer
2 identification number or other unique identifier
3 of the entity impacted by the covered cyber inci-
4 dent.

5 “(F) Contact information, such as tele-
6 phone number or electronic mail address, that
7 the Office may use to contact the covered entity
8 or an authorized agent of such covered entity,
9 or, where applicable, the service provider of
10 such covered entity acting with the express per-
11 mission, and at the direction, of the covered en-
12 tity to assist with compliance with the require-
13 ments of this subtitle.

14 “(5) A clear description of the specific required
15 contents of a report pursuant to subsection (a)(2),
16 which shall be the following information, to the ex-
17 tent applicable and available, with respect to a ran-
18 som payment:

19 “(A) A description of the ransomware at-
20 tack, including the estimated date range of the
21 attack.

22 “(B) Where applicable, a description of the
23 vulnerabilities, tactics, techniques, and proce-
24 dures used to perpetuate the ransomware at-
25 tack.

1 “(C) Where applicable, any identifying or
2 contact information related to the actor or ac-
3 tors reasonably believed to be responsible for
4 the ransomware attack.

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

8 “(E) Contact information, such as tele-
9 phone number or electronic mail address, that
10 the Office may use to contact the entity that
11 made the ransom payment or an authorized
12 agent of such covered entity, or, where applica-
13 ble, the service provider of such covered entity
14 acting with the express permission, and at the
15 direction of, that entity to assist with compli-
16 ance with the requirements of this subtitle.

17 “(F) The date of the ransom payment.

18 “(G) The ransom payment demand, includ-
19 ing the type of virtual currency or other com-
20 modity requested, if applicable.

21 “(H) The ransom payment instructions,
22 including information regarding where to send
23 the payment, such as the virtual currency ad-
24 dress or physical address the funds were re-
25 quested to be sent to, if applicable.

1 “(I) The amount of the ransom payment.

2 “(J) A summary of the due diligence re-
3 view required under subsection (e).

4 “(6) A clear description of the types of data re-
5 quired to be preserved pursuant to subsection (a)(4)
6 and the period of time for which the data is required
7 to be preserved.

8 “(7) Deadlines for submitting reports to the Di-
9 rector required under subsection (a)(3), which
10 shall—

11 “(A) be established by the Director in con-
12 sultation with the Council;

13 “(B) consider any existing regulatory re-
14 porting requirements similar in scope, purpose,
15 and timing to the reporting requirements to
16 which such a covered entity may also be sub-
17 ject, and make efforts to harmonize the timing
18 and contents of any such reports to the max-
19 imum extent practicable; and

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

23 “(8) Procedures for—

24 “(A) entities to submit reports required by
25 paragraphs (1), (2), and (3) of subsection (a),

1 which shall include, at a minimum, a concise,
2 user-friendly web-based form;

3 “(B) the Office to carry out the enforce-
4 ment provisions of section 2233, including with
5 respect to the issuance of subpoenas and other
6 aspects of noncompliance;

7 “(C) implementing the exceptions provided
8 in subparagraphs (A), (B), and (D) of sub-
9 section (a)(5); and

10 “(D) anonymizing and safeguarding infor-
11 mation received and disclosed through covered
12 cyber incident reports and ransom payment re-
13 ports that is known to be personal information
14 of a specific individual or information that iden-
15 tifies a specific individual that is not directly re-
16 lated to a cybersecurity threat.

17 “(d) THIRD-PARTY REPORT SUBMISSION AND RAN-
18 SOM PAYMENT.—

19 “(1) REPORT SUBMISSION.—An entity, includ-
20 ing a covered entity, that is required to submit a
21 covered cyber incident report or a ransom payment
22 report may use a third party, such as an incident re-
23 sponse company, insurance provider, service pro-
24 vider, information sharing and analysis organization,

1 or law firm, to submit the required report under
2 subsection (a).

3 “(2) RANSOM PAYMENT.—If an entity impacted
4 by a ransomware attack uses a third party to make
5 a ransom payment, the third party shall not be re-
6 quired to submit a ransom payment report for itself
7 under subsection (a)(2).

8 “(3) DUTY TO REPORT.—Third-party reporting
9 under this subparagraph does not relieve a covered
10 entity or an entity that makes a ransom payment
11 from the duty to comply with the requirements for
12 covered cyber incident report or ransom payment re-
13 port submission.

14 “(4) RESPONSIBILITY TO ADVISE.—Any third
15 party used by an entity that knowingly makes a ran-
16 som payment on behalf of an entity impacted by a
17 ransomware attack shall advise the impacted entity
18 of the responsibilities of the impacted entity regard-
19 ing a due diligence review under subsection (e) and
20 reporting ransom payments under this section.

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

1 tity or entity shall conduct a due diligence review of alter-
2 natives to making the ransom payment, including an anal-
3 ysis of whether the covered entity or entity can recover
4 from the ransomware attack through other means.

5 “(f) OUTREACH TO COVERED ENTITIES.—

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

14 “(2) ELEMENTS.—The outreach and education
15 campaign under paragraph (1) shall include the fol-
16 lowing:

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

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

23 “(C) An overview of the protections af-
24 farded to covered entities for complying with

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

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

7 “(E) Specific outreach to cybersecurity
8 vendors, incident response providers, cybersecu-
9 rity insurance entities, and other entities that
10 may support covered entities or ransomware at-
11 tack victims.

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

14 “(3) COORDINATION.—In conducting the out-
15 reach and education campaign required under para-
16 graph (1), the Director may coordinate with—

17 “(A) the Critical Infrastructure Partner-
18 ship Advisory Council established under section
19 871;

20 “(B) information sharing and analysis or-
21 ganizations;

22 “(C) trade associations;

23 “(D) information sharing and analysis cen-
24 ters;

25 “(E) sector coordinating councils; and

1 “(F) any other entity as determined appro-
2 priate by the Director.

3 “(g) EVALUATION OF STANDARDS.—

4 “(1) IN GENERAL.—Before issuing the final
5 rule pursuant to subsection (b)(2), the Director shall
6 review the data collected by the Office, and in con-
7 sultation with other appropriate entities, assess the
8 effectiveness of the rule with respect to—

9 “(A) the number of reports received;

10 “(B) the utility of the reports received;

11 “(C) the number of supplemental reports
12 required to be submitted; and

13 “(D) any other factor determined appro-
14 priate by the Director.

15 “(2) SUBMISSION TO CONGRESS.—The Director
16 shall submit to the Committee on Homeland Secu-
17 rity and Governmental Affairs of the Senate and the
18 Committee on Homeland Security of the House of
19 Representatives the results of the evaluation de-
20 scribed in paragraph (1) and may thereafter, in ac-
21 cordance with the requirements under subsection
22 (b), publish in the Federal Register a final rule im-
23 plementing this section.

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

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

6 **“SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER IN-**
7 **CIDENTS.**

8 “(a) IN GENERAL.—Entities may voluntarily report
9 incidents or ransom payments to the Director that are not
10 required under paragraph (1), (2), or (3) of section
11 2232(a), but may enhance the situational awareness of
12 cyber threats.

13 “(b) VOLUNTARY PROVISION OF ADDITIONAL INFOR-

14 MATION IN REQUIRED REPORTS.—Entities may volun-

15 tarily include in reports required under paragraph (1), (2),

16 or (3) of section 2232(a) information that is not required

17 to be included, but may enhance the situational awareness

18 of cyber threats.

19 “(c) APPLICATION OF PROTECTIONS.—The protec-

20 tions under section 2235 applicable to covered cyber inci-

21 dent reports shall apply in the same manner and to the

22 same extent to reports and information submitted under

23 subsections (a) and (b).

1 **“SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.**

2 “(a) PURPOSE.—In the event that an entity that is
3 required to submit a report under section 2232(a) fails
4 to comply with the requirement to report, the Director
5 may obtain information about the incident or ransom pay-
6 ment by engaging the entity directly to request informa-
7 tion about the incident or ransom payment, and if the Di-
8 rector is unable to obtain information through such en-
9 gagement, by issuing a subpoena to the entity, pursuant
10 to subsection (c), to gather information sufficient to deter-
11 mine whether a covered cyber incident or ransom payment
12 has occurred, and, if so, whether additional action is war-
13 ranted pursuant to subsection (d).

14 “(b) INITIAL REQUEST FOR INFORMATION.—

15 “(1) IN GENERAL.—If the Director has reason
16 to believe, whether through public reporting or other
17 information in the possession of the Federal Govern-
18 ment, including through analysis performed pursu-
19 ant to paragraph (1) or (2) of section 2231(b), that
20 an entity has experienced a covered cyber incident or
21 made a ransom payment but failed to report such
22 incident or payment to the Office within 72 hours in
23 accordance to section 2232(a), the Director shall re-
24 quest additional information from the entity to con-
25 firm whether or not a covered cyber incident or ran-
26 som payment has occurred.

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

5 “(c) AUTHORITY TO ISSUE SUBPOENAS AND
6 DEBAR.—

7 “(1) IN GENERAL.—If, after the date that is 72
8 hours from the date on which the Director made the
9 request for information in subsection (b), the Direc-
10 tor has received no response from the entity from
11 which such information was requested, or received
12 an inadequate response, the Director may issue to
13 such entity a subpoena to compel disclosure of infor-
14 mation the Director deems necessary to determine
15 whether a covered cyber incident or ransom payment
16 has occurred.

17 “(2) CIVIL ACTION.—

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

23 “(B) VENUE.—An action under this para-
24 graph may be brought in the judicial district in

1 which the entity against which the action is
2 brought resides, is found, or does business.

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

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

10 “(4) DEBARMENT OF FEDERAL CONTRAC-
11 TORS.—If a covered entity with a Federal Govern-
12 ment contract, grant, or cooperative agreement fails
13 to comply with a subpoena issued under this sub-
14 section—

15 “(A) the Director may refer the matter to
16 the Administrator of General Services; and

17 “(B) upon receiving a referral from the Di-
18 rector, the Administrator of General Services
19 may impose additional available penalties, in-
20 cluding suspension or debarment.

21 “(d) PROVISION OF CERTAIN INFORMATION TO AT-
22 TORNEY GENERAL.—

23 “(1) IN GENERAL.—Notwithstanding section
24 2235(a) and subsection (b)(2) of this section, if the
25 Director determines, based on the information pro-

1 vided in response to the subpoena issued pursuant to
2 subsection (c), that the facts relating to the covered
3 cyber incident or ransom payment at issue may con-
4 stitute grounds for a regulatory enforcement action
5 or criminal prosecution, the Director may provide
6 that information to the Attorney General or the ap-
7 propriate regulator, who may use that information
8 for a regulatory enforcement action or criminal pros-
9 ecution.

10 “(2) APPLICATION TO CERTAIN ENTITIES AND
11 THIRD PARTIES.—A covered cyber incident or ran-
12 som payment report submitted to the Office by an
13 entity that makes a ransom payment or third party
14 under section 2232 shall not be used by any Fed-
15 eral, State, Tribal, or local government to investigate
16 or take another law enforcement action against the
17 entity that makes a ransom payment or third party.

18 “(3) RULE OF CONSTRUCTION.—Nothing in
19 this subtitle shall be construed to provide an entity
20 that submits a covered cyber incident report or ran-
21 som payment report under section 2232 any immu-
22 nity from law enforcement action for making a ran-
23 som payment otherwise prohibited by law.

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

4 “(1) the size and complexity of the entity;

5 “(2) the complexity in determining if a covered
6 cyber incident has occurred;

7 “(3) prior interaction with the Agency or
8 awareness of the entity of the policies and proce-
9 dures of the Agency for reporting covered cyber inci-
10 dents and ransom payments; and

11 “(4) for non-covered entities required to submit
12 a ransom payment report, the ability of the entity to
13 perform a due diligence review pursuant to section
14 2232(e).

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

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

20 “(1) issued an initial request for information
21 pursuant to subsection (b);

22 “(2) issued a subpoena pursuant to subsection
23 (c);

24 “(3) brought a civil action pursuant to sub-
25 section (c)(2); or

1 “(4) conducted additional actions pursuant to
2 subsection (d).

3 **“SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO**
4 **THE FEDERAL GOVERNMENT.**

5 “(a) DISCLOSURE, RETENTION, AND USE.—

6 “(1) AUTHORIZED ACTIVITIES.—Information
7 provided to the Office or Agency pursuant to section
8 2232 may be disclosed to, retained by, and used by,
9 consistent with otherwise applicable provisions of
10 Federal law, any Federal agency or department,
11 component, officer, employee, or agent of the Fed-
12 eral Government solely for—

13 “(A) a cybersecurity purpose;

14 “(B) the purpose of identifying—

15 “(i) a cyber threat, including the
16 source of the cyber threat; or

17 “(ii) a security vulnerability;

18 “(C) the purpose of responding to, or oth-
19 erwise preventing or mitigating, a specific
20 threat of death, a specific threat of serious bod-
21 ily harm, or a specific threat of serious eco-
22 nomic harm, including a terrorist act or a use
23 of a weapon of mass destruction;

24 “(D) the purpose of responding to, inves-
25 tigating, prosecuting, or otherwise preventing or

1 mitigating, a serious threat to a minor, includ-
2 ing sexual exploitation and threats to physical
3 safety; or

4 “(E) the purpose of preventing, inves-
5 tigating, disrupting, or prosecuting an offense
6 arising out of a covered cyber incident or any
7 of the offenses listed in section 105(d)(5)(A)(v)
8 of the Cybersecurity Act of 2015 (6 U.S.C.
9 1504(d)(5)(A)(v)).

10 “(2) AGENCY ACTIONS AFTER RECEIPT.—

11 “(A) RAPID, CONFIDENTIAL SHARING OF
12 CYBER THREAT INDICATORS.—Upon receiving a
13 covered cyber incident or ransom payment re-
14 port submitted pursuant to this section, the Of-
15 fice shall immediately review the report to de-
16 termine whether the incident that is the subject
17 of the report is connected to an ongoing cyber
18 threat or security vulnerability and where appli-
19 cable, use such report to identify, develop, and
20 rapidly disseminate to appropriate stakeholders
21 actionable, anonymized cyber threat indicators
22 and defensive measures.

23 “(B) STANDARDS FOR SHARING SECURITY
24 VULNERABILITIES.—With respect to informa-
25 tion in a covered cyber incident or ransom pay-

1 ment report regarding a security vulnerability
2 referred to in paragraph (1)(B)(ii), the Director
3 shall develop principles that govern the timing
4 and manner in which information relating to se-
5 curity vulnerabilities may be shared, consistent
6 with common industry best practices and
7 United States and international standards.

8 “(3) PRIVACY AND CIVIL LIBERTIES.—Informa-
9 tion contained in covered cyber incident and ransom
10 payment reports submitted to the Office pursuant to
11 section 2232 shall be retained, used, and dissemi-
12 nated, where permissible and appropriate, by the
13 Federal Government in accordance with processes to
14 be developed for the protection of personal informa-
15 tion adopted pursuant to section 105 of the Cyberse-
16 curity Act of 2015 (6 U.S.C. 1504) and in a manner
17 that protects from unauthorized use or disclosure
18 any information that may contain—

19 “(A) personal information of a specific in-
20 dividual; or

21 “(B) information that identifies a specific
22 individual that is not directly related to a cyber-
23 security threat.

24 “(4) DIGITAL SECURITY.—The Office shall en-
25 sure that reports submitted to the Office pursuant

1 to section 2232, and any information contained in
2 those reports, are collected, stored, and protected at
3 a minimum in accordance with the requirements for
4 moderate impact Federal information systems, as
5 described in Federal Information Processing Stand-
6 ards Publication 199, or any successor document.

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

15 “(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—
16 The submission of a report under section 2232 to the Of-
17 fice shall not constitute a waiver of any applicable privilege
18 or protection provided by law, including trade secret pro-
19 tection and attorney-client privilege.

20 “(c) EXEMPTION FROM DISCLOSURE.—Information
21 contained in a report submitted to the Office under section
22 2232 shall be exempt from disclosure under section
23 552(b)(3)(B) of title 5, United States Code (commonly
24 known as the ‘Freedom of Information Act’) and any

1 State, Tribal, or local provision of law requiring disclosure
2 of information or records.

3 “(d) EX PARTE COMMUNICATIONS.—The submission
4 of a report to the Agency under section 2232 shall not
5 be subject to a rule of any Federal agency or department
6 or any judicial doctrine regarding ex parte communica-
7 tions with a decision-making official.

8 “(e) LIABILITY PROTECTIONS.—

9 “(1) IN GENERAL.—No cause of action shall lie
10 or be maintained in any court by any person or enti-
11 ty and any such action shall be promptly dismissed
12 for the submission of a report pursuant to section
13 2232(a) that is submitted in conformance with this
14 subtitle and the rules promulgated under section
15 2232(b), except that this subsection shall not apply
16 with regard to an action by the Federal Government
17 pursuant to section 2234(c)(2).

18 “(2) SCOPE.—The liability protections provided
19 in subsection (e) shall only apply to or affect litiga-
20 tion that is solely based on the submission of a cov-
21 ered cyber incident report or ransom payment report
22 to the Office, and nothing in this subtitle shall cre-
23 ate a defense to a discovery request, or otherwise
24 limit or affect the discovery of information from a

1 cause of action authorized under any Federal, State,
2 local, or Tribal law.

3 “(f) SHARING WITH FEDERAL AND NON-FEDERAL
4 ENTITIES.—The Agency shall anonymize the victim who
5 reported the information when making information pro-
6 vided in reports received under section 2232 available to
7 critical infrastructure owners and operators and the gen-
8 eral public.

9 “(g) PROPRIETARY INFORMATION.—Information
10 contained in a report submitted to the Agency under sec-
11 tion 2232 shall be considered the commercial, financial,
12 and proprietary information of the covered entity when so
13 designated by the covered entity.”.

14 (c) TECHNICAL AND CONFORMING AMENDMENT.—
15 The table of contents in section 1(b) of the Homeland Se-
16 curity Act of 2002 (Public Law 107–296; 116 Stat. 2135)
17 is amended by inserting after the items relating to subtitle
18 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. 2233. Voluntary reporting of other cyber incidents.

“Sec. 2234. Noncompliance with required reporting.

“Sec. 2235. Information shared with or provided to the Federal Government.”.

19 **SEC. 4. FEDERAL SHARING OF INCIDENT REPORTS.**

20 (a) CYBER INCIDENT REPORTING SHARING.—Not-
21 withstanding any other provision of law or regulation, any
22 Federal agency that receives a report from an entity of

1 a cyber attack, including a ransomware attack, shall pro-
2 vide all such information to the Director of the Cybersecu-
3 rity Infrastructure Security Agency not later than 24
4 hours after receiving the report, unless a shorter period
5 is required by an agreement made between the Cyber Inci-
6 dent Review Office established under section 2231 of the
7 Homeland Security Act of 2002, as added by section 3(b)
8 of this Act, and another Federal entity.

9 (b) CREATION OF COUNCIL.—Section 1752(c)(1) of
10 the William M. (Mac) Thornberry National Defense Au-
11 thorization Act for Fiscal Year 2021 (6 U.S.C.
12 1500(c)(1)) is amended—

13 (1) in subparagraph (G), by striking “and” at
14 the end;

15 (2) by redesignating subparagraph (H) as sub-
16 paragraph (I); and

17 (3) by inserting after subparagraph (G) the fol-
18 lowing:

19 “(H) lead an intergovernmental Cyber In-
20 cident Reporting Council, in coordination with
21 the Director of the Office of Management and
22 Budget and the Director of the Cybersecurity
23 and Infrastructure Security Agency and in con-
24 sultation with Sector Risk Management Agen-
25 cies (as defined in section 2201 of the Home-

1 land Security Act of 2002 (6 U.S.C. 651)) and
2 other appropriate Federal agencies, to coordi-
3 nate, deconflict, and harmonize Federal incident
4 reporting requirements, including those issued
5 through regulations, for covered entities (as de-
6 fined in section 2230 of such Act) and entities
7 that make a ransom payment (as defined in
8 such section 2201 (6 U.S.C. 651)); and”.

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

17 (1) review existing regulatory requirements, in-
18 cluding the information required in such reports, to
19 report cyber incidents and ensure that any such re-
20 porting requirements and procedures avoid con-
21 flicting, duplicative, or burdensome requirements;
22 and

23 (2) coordinate with the Director and regulatory
24 authorities that receive reports relating to cyber inci-
25 dents to identify opportunities to streamline report-

1 ing processes, and where feasible, facilitate inter-
2 agency agreements between such authorities to per-
3 mit the sharing of such reports, consistent with ap-
4 plicable law and policy, without impacting the ability
5 of such agencies to gain timely situational awareness
6 of a covered cyber incident or ransom payment.

7 **SEC. 5. RANSOMWARE VULNERABILITY WARNING PILOT**
8 **PROGRAM.**

9 (a) PROGRAM.—Not less than 90 days after the date
10 of enactment of this Act, the Director shall establish a
11 ransomware vulnerability warning program to leverage ex-
12 isting authorities and technology to specifically develop
13 processes and procedures, and to dedicate resources, to
14 identifying information systems that contain security
15 vulnerabilities associated with common ransomware at-
16 tacks, and to notify the owners of those vulnerable systems
17 of their security vulnerability.

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

20 (1) identify the most common security vulnera-
21 bilities utilized in ransomware attacks and mitiga-
22 tion techniques; and

23 (2) utilize existing authorities to identify Fed-
24 eral and other relevant information systems that

1 contain the security vulnerabilities identified in para-
2 graph (1).

3 (c) ENTITY NOTIFICATION.—

4 (1) IDENTIFICATION.—If the Director is able to
5 identify the entity at risk that owns or operates a
6 vulnerable information system identified in sub-
7 section (b), the Director may notify the owner of the
8 information system.

9 (2) NO IDENTIFICATION.—If the Director is not
10 able to identify the entity at risk that owns or oper-
11 ates a vulnerable information system identified in
12 subsection (b), the Director may utilize the subpoena
13 authority pursuant to section 2209 of the Homeland
14 Security Act of 2002 (6 U.S.C. 659) to identify and
15 notify the entity at risk pursuant to the procedures
16 within that section.

17 (3) REQUIRED INFORMATION.—A notification
18 made under paragraph (1) shall include information
19 on the identified security vulnerability and mitiga-
20 tion techniques.

21 (d) PRIORITIZATION OF NOTIFICATIONS.—To the ex-
22 tent practical, the Director shall prioritize covered entities
23 for identification and notification activities under the pilot
24 program established under this section.

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

7 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
8 tion shall be construed to provide additional authorities
9 to the Director to identify vulnerabilities or vulnerable sys-
10 tems.

11 **SEC. 6. RANSOMWARE THREAT MITIGATION ACTIVITIES.**

12 (a) JOINT RANSOMWARE TASK FORCE.—

13 (1) IN GENERAL.—Not later than 180 days
14 after the date of enactment of this section, the Na-
15 tional Cyber Director shall establish and chair the
16 Joint Ransomware Task Force to coordinate an on-
17 going, nationwide campaign against ransomware at-
18 tacks, and identify and pursue opportunities for
19 international cooperation.

20 (2) COMPOSITION.—The Joint Ransomware
21 Task Force shall consist of participants from Fed-
22 eral agencies, as determined appropriate by the Na-
23 tional Cyber Director in consultation with the Sec-
24 retary of Homeland Security.

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

5 (A) Prioritization of intelligence-driven op-
6 erations to disrupt specific ransomware actors.

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

12 (C) Identifying, in consultation with rel-
13 evant entities, a list of highest threat ransom-
14 ware entities updated on an ongoing basis, in
15 order to facilitate—

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

18 (ii) identify metrics for success of said
19 actions.

20 (D) Disrupting ransomware criminal ac-
21 tors, associated infrastructure, and their fi-
22 nances.

23 (E) Facilitating coordination and collabo-
24 ration between Federal entities and relevant en-

1 tities, including the private sector, to improve
2 Federal actions against ransomware threats.

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

5 (G) Creation of after-action reports and
6 other lessons learned from Federal actions that
7 identify successes and failures to improve sub-
8 sequent actions.

9 (H) Any other activities determined appro-
10 priate by the task force to mitigate the threat
11 of ransomware attacks against Federal and
12 non-Federal entities.

13 (b) CLARIFYING PRIVATE-SECTOR LAWFUL DEFEN-
14 SIVE MEASURES.—Not later than 180 days after the date
15 of enactment of this Act, the National Cyber Director, in
16 coordination with the Secretary of Homeland Security and
17 the Attorney General, shall submit to the Committee on
18 Homeland Security and Governmental Affairs and the
19 Committee on the Judiciary of the Senate and the Com-
20 mittee on Homeland Security, the Committee on the Judi-
21 ciary, and the Committee on Oversight and Reform of the
22 House of Representatives a report that describes defensive
23 measures that private-sector actors can take when coun-
24 tering ransomware attacks and what laws need to be clari-
25 fied to enable that action.

1 (c) RULE OF CONSTRUCTION.—Nothing in this sec-
2 tion shall be construed as providing any additional author-
3 ity to any Federal agency.

4 **SEC. 7. CONGRESSIONAL REPORTING.**

5 (a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not
6 later than 30 days after the date on which the Director
7 issues the interim final rule under section 2232(b)(1) of
8 the Homeland Security Act of 2002, as added by section
9 3(b) of this Act, the Director shall submit to the Com-
10 mittee on Homeland Security and Governmental Affairs
11 of the Senate and the Committee on Homeland Security
12 of the House of Representatives a report that describes
13 how the Director engaged stakeholders in the development
14 of the interim final rule.

15 (b) REPORT ON OPPORTUNITIES TO STRENGTHEN
16 SECURITY RESEARCH.—Not later than 1 year after the
17 date of enactment of this Act, the Director shall submit
18 to the Committee on Homeland Security and Govern-
19 mental Affairs of the Senate and the Committee on Home-
20 land Security of the House of Representatives a report de-
21 scribing how the Cyber Incident Review Office has carried
22 out activities under section 2231(b)(9) of the Homeland
23 Security Act of 2002, as added by section 3(b) of this Act,
24 by proactively identifying opportunities to use cyber inci-

1 dent data to inform and enabling cybersecurity research
2 within the academic and private sector.

3 (c) REPORT ON RANSOMWARE VULNERABILITY
4 WARNING PILOT PROGRAM.—Not later than 1 year after
5 the date of enactment of this Act, and annually thereafter
6 for the duration of the pilot program established under
7 section 5, the Director shall submit to the Committee on
8 Homeland Security and Governmental Affairs of the Sen-
9 ate and the Committee on Homeland Security of the
10 House of Representatives a report, which may include a
11 classified annex, on the effectiveness of the pilot program,
12 which shall include a discussion of the following:

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

16 (2) The identification of most common vulnera-
17 bilities utilized in ransomware.

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

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

23 (d) REPORT ON HARMONIZATION OF REPORTING
24 REGULATIONS.—Not later than 180 days after the date
25 on which the National Cyber Director convenes the Coun-

1 cil described in section 1752(c)(1)(H) of the William M.
2 (Mac) Thornberry National Defense Authorization Act for
3 Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National
4 Cyber Director shall submit to the appropriate congress-
5 sional committees a report that includes—

6 (1) a list of duplicative Federal cyber incident
7 reporting requirements on covered entities and enti-
8 ties that make a ransom payment;

9 (2) any actions the National Cyber Director in-
10 tends to take to harmonize the duplicative reporting
11 requirements; and

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

14 (e) GAO REPORT.—Not later than 2 years after the
15 date of enactment of this Act, the Comptroller General
16 of the United States shall submit to the Committee on
17 Homeland Security and Governmental Affairs of the Sen-
18 ate and the Committee on Homeland Security of the
19 House of Representatives a report on the implementation
20 of this Act and the amendments made by this Act.

○