

Calendar No. 633117TH CONGRESS
2^D SESSION**S. 2875****[Report No. 117-249]**

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

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 28, 2021

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

DECEMBER 13, 2022

Reported by Mr. PETERS, with an amendment

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

A BILL

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

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

1 **SECTION 1. SHORT TITLE.**

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

4 **SEC. 2. DEFINITIONS.**

5 In this Act:

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

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

18 (3) ~~DIRECTOR.~~—The term “Director” means
19 the Director of the Cybersecurity and Infrastructure
20 Security Agency.

21 (4) ~~INFORMATION SYSTEM; SECURITY VULNER-~~
22 ~~ABILITY.~~—The terms “information system” and “se-
23 curity vulnerability” have the meanings given those
24 terms in section 102 of the Cybersecurity Act of
25 2015 (6 U.S.C. 1501).

1 **SEC. 3. CYBER INCIDENT REPORTING.**

2 (a) **DEFINITIONS.**—

3 (1) **IN GENERAL.**—Section 2201 of the Home-
4 land Security Act of 2002 (6 U.S.C. 651) is amend-
5 ed—

6 (A) by redesignating paragraphs (1), (2),
7 (3), (4), (5), and (6) as paragraphs (2), (4),
8 (5), (7), (10), and (11), respectively;

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

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

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

20 “(3) **CYBER ATTACK.**—The term ‘cyber attack’
21 means the use of unauthorized or malicious code on
22 an information system, or the use of another digital
23 mechanism such as a denial of service attack, to in-
24 terrupt or disrupt the operations of an information
25 system or compromise the confidentiality, avail-

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

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

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

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

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

20 “(9) **RANSOMWARE ATTACK.**—The term ‘ran-
 21 somware attack’—

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

1 nial of service attack, to interrupt or disrupt
2 the operations of an information system or com-
3 promise the confidentiality, availability, or in-
4 tegrity of electronic data stored on, processed
5 by, or transiting an information system to ex-
6 tort a demand for a ransom payment; and

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

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

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

23 “(14) VIRTUAL CURRENCY.—The term ‘virtual
24 currency’ means the digital representation of value

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

3 “(15) VIRTUAL CURRENCY ADDRESS.—The
4 term ‘virtual currency address’ means a unique pub-
5 lic cryptographic key identifying the location to
6 which a virtual currency payment can be made.”.

7 (2) CONFORMING AMENDMENT.—Section
8 9002(A)(7) of the William M. (Mac) Thornberry Na-
9 tional Defense Authorization Act for Fiscal Year
10 2021 (6 U.S.C. 652a(a)(7)) is amended to read as
11 follows:

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

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

19 **“Subtitle C—Cyber Incident**
20 **Reporting**

21 **“SEC. 2230. DEFINITIONS.**

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

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

1 “~~(1) COUNCIL.~~—The term ‘Council’ means the
2 Cyber Incident Reporting Council described in sec-
3 tion ~~1752(e)(1)(H)~~ of the William M. (Mac) Thorn-
4 berry National Defense Authorization Act for Fiscal
5 Year 2021 (6 U.S.C. ~~1500(e)(1)(H)~~).

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

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

17 “~~(4) CYBER INCIDENT.~~—The term ‘cyber inci-
18 dent’ has the meaning given the term ‘incident’ in
19 section ~~2209(a)~~.

20 “~~(5) CYBER THREAT.~~—The term ‘cyber
21 threat’—

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

1 “(B) does not include any activity related
2 to good faith security research, including par-
3 ticipation in a bug-bounty program or a vulner-
4 ability disclosure program.

5 “(6) CYBER THREAT INDICATOR; CYBERSECU-
6 RITY PURPOSE; DEFENSIVE MEASURE; FEDERAL EN-
7 TITY; INFORMATION SYSTEM; SECURITY CONTROL;
8 SECURITY VULNERABILITY.—The terms ‘cyber
9 threat indicator’, ‘cybersecurity purpose’, ‘defensive
10 measure’, ‘Federal entity’, ‘information system’, ‘se-
11 curity control’, and ‘security vulnerability’ have the
12 meanings given those terms in section 102 of the
13 Cybersecurity Act of 2015 (6 U.S.C. 1501).

14 “(7) SMALL BUSINESS.—The term ‘small busi-
15 ness’—

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

19 “(B) does not include—

20 “(i) a business that is a covered enti-
21 ty; or

22 “(ii) a business that holds a govern-
23 ment contract, unless that contractor is a
24 party only to—

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

3 “(II) a contract to provide prod-
4 ucts or services unrelated to informa-
5 tion technology that is below the
6 micro-purchase threshold, as defined
7 in section 2.101 of title 48, Code of
8 Federal Regulations, or any successor
9 regulation.

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

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

21 “(b) ACTIVITIES.—The Office shall, in furtherance of
22 the activities specified in sections 2202(e), 2203, and
23 2209(e)—

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

1 security Information Sharing Act of 2015 (6 U.S.C.
2 1501 et seq.) reports from covered entities related to
3 a covered cyber incident to assess the effectiveness
4 of security controls and identify tactics, techniques,
5 and procedures adversaries use to overcome those
6 controls;

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

13 “(3) leverage information gathered about cyber-
14 security incidents to—

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

22 “(B) provide appropriate entities, including
23 agencies, sector coordinating councils, informa-
24 tion sharing and analysis organizations, tech-
25 nology providers, cybersecurity and incident re-

1 sponse firms, and security researchers, with
2 timely, actionable, and anonymized reports of
3 cyber attack campaigns and trends, including,
4 to the maximum extent practicable, related con-
5 textual information, cyber threat indicators, and
6 defensive measures;

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

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

20 “(6) for a covered cyber incident, including a
21 ransomware attack, that also satisfies the definition
22 of a substantial cyber incident, or is part of a group
23 of related cyber incidents that together satisfy such
24 definition, conduct a review of the details sur-
25 rounding the covered cyber incident or group of

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

3 “(7) with respect to covered cyber incident re-
4 ports under subsection (e) involving an ongoing
5 cyber threat or security vulnerability, immediately
6 review those reports for cyber threat indicators that
7 can be anonymized and disseminated, with defensive
8 measures, to appropriate stakeholders, in coordina-
9 tion with other divisions within the Agency, as ap-
10 propriate;

11 “(8) publish quarterly unclassified, public re-
12 ports that may be based on the unclassified informa-
13 tion contained in the reports required under sub-
14 section (e);

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

21 “(10) proactively identify opportunities, con-
22 sistent with the protections in section 2235, to lever-
23 age and utilize data on cyber incidents in a manner
24 that enables and strengthens cybersecurity research
25 carried out by academic institutions and other pri-

1 vate sector organizations, to the greatest extent
2 practicable;

3 “(11) on a not less frequently than annual
4 basis, analyze public disclosures made pursuant to
5 parts 229 and 249 of title 17, Code of Federal Reg-
6 ulations, or any subsequent document submitted to
7 the Securities and Exchange Commission by entities
8 experiencing cyber incidents and compare such dis-
9 closures to reports received by the Office; and

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

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

1 minority leader of the House of Representatives, the Com-
2 mittee on Homeland Security and Governmental Affairs
3 of the Senate, and the Committee on Homeland Security
4 of the House of Representatives a report that character-
5 izes the cyber threat facing Federal agencies and covered
6 entities, including applicable intelligence and law enforce-
7 ment information, covered cyber incidents, and ransom-
8 ware attacks, as of the date of the report, which shall—

9 “(1) include the total number of reports sub-
10 mitted under sections 2232 and 2233 during the
11 preceding month, including a breakdown of required
12 and voluntary reports;

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

19 “(A) the infrastructure, tactics, and tech-
20 niques malicious cyber actors commonly use;
21 and

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

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

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

6 “(d) ORGANIZATION.—The Director may organize
7 the Office within the Agency as the Director deems appro-
8 priate, including harmonizing the functions of the Office
9 with other authorized activities.

10 “**SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER IN-**
11 **CIDENTS.**

12 “(a) IN GENERAL.—

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

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

1 “(3) SUPPLEMENTAL REPORTS.—A covered en-
2 tity shall promptly submit to the Director an update
3 or supplement to a previously submitted covered
4 cyber incident report if new or different information
5 becomes available or if the covered entity makes a
6 ransom payment after submitting a covered cyber in-
7 cident report required under paragraph (1).

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

14 “(5) EXCEPTIONS.—

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

1 “(B) SUBSTANTIALLY SIMILAR REPORTED
2 INFORMATION.—The requirements under para-
3 graphs (1), (2), and (3) shall not apply to an
4 entity required by law, regulation, or contract
5 to report substantially similar information to
6 another Federal agency within a substantially
7 similar timeframe.

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

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

24 “(b) RULEMAKING.—

1 “(1) INTERIM FINAL RULE.—Not later than
2 270 days after the date of enactment of this section,
3 and after a 60-day consultative period, followed by
4 a 90-day comment period with appropriate stake-
5 holders, the Director, in consultation with Sector
6 Risk Management Agencies and the heads of other
7 Federal agencies, shall publish in the Federal Reg-
8 ister an interim final rule to implement subsection
9 (a).

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

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

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

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

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

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

10 “(C) the extent to which damage, disrup-
11 tion, or unauthorized access to such an entity,
12 including the accessing of sensitive cybersecu-
13 rity vulnerability information or penetration
14 testing tools or techniques, will likely enable the
15 disruption of the reliable operation of critical
16 infrastructure.

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

20 “(A) at a minimum, require the occurrence
21 of—

22 “(i) the unauthorized access to an in-
23 formation system or network with a sub-
24 stantial loss of confidentiality, integrity, or
25 availability of such information system or

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

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

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

13 “(B) consider—

14 “(i) the sophistication or novelty of
15 the tactics used to perpetrate such an inci-
16 dent, as well as the type, volume, and sen-
17 sitivity of the data at issue;

18 “(ii) the number of individuals di-
19 rectly or indirectly affected or potentially
20 affected by such an incident; and

21 “(iii) potential impacts on industrial
22 control systems, such as supervisory con-
23 trol and data acquisition systems, distrib-
24 uted control systems, and programmable
25 logic controllers; and

1 “(C) exclude—

2 “(i) any event where the cyber inci-
3 dent is perpetuated by a United States
4 Government entity, good-faith security re-
5 search, or in response to an invitation by
6 the owner or operator of the information
7 system for third parties to find vulnerabili-
8 ties in the information system, such as
9 through a vulnerability disclosure program
10 or the use of authorized penetration test-
11 ing services; and

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

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

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

1 “(A) A description of the covered cyber in-
2 cident, including—

3 “(i) identification and a description of
4 the function of the affected information
5 systems, networks, or devices that were, or
6 are reasonably believed to have been, af-
7 fected by such incident;

8 “(ii) a description of the unauthorized
9 access with substantial loss of confiden-
10 tiality, integrity, or availability of the af-
11 fected information system or network or
12 disruption of business or industrial oper-
13 ations;

14 “(iii) the estimated date range of such
15 incident; and

16 “(iv) the impact to the operations of
17 the covered entity.

18 “(B) Where applicable, a description of the
19 vulnerabilities, tactics, techniques, and proce-
20 dures used to perpetuate the covered cyber inci-
21 dent.

22 “(C) Where applicable, any identifying or
23 contact information related to each actor rea-
24 sonably believed to be responsible for such inci-
25 dent.

1 “(D) Where applicable, identification of
2 the category or categories of information that
3 was, or is reasonably believed to have been,
4 accessed or acquired by an unauthorized per-
5 son.

6 “(E) The name and, if applicable, taxpayer
7 identification number or other unique identifier
8 of the entity impacted by the covered cyber inci-
9 dent.

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

19 “(5) A clear description of the specific required
20 contents of a report pursuant to subsection (a)(2),
21 which shall be the following information, to the ex-
22 tent applicable and available, with respect to a ran-
23 som payment:

1 “(A) A description of the ransomware at-
2 tack, including the estimated date range of the
3 attack.

4 “(B) Where applicable, a description of the
5 vulnerabilities, tactics, techniques, and proce-
6 dures used to perpetuate the ransomware at-
7 tack.

8 “(C) Where applicable, any identifying or
9 contact information related to the actor or ac-
10 tors reasonably believed to be responsible for
11 the ransomware attack.

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

15 “(E) Contact information, such as tele-
16 phone number or electronic mail address, that
17 the Office may use to contact the entity that
18 made the ransom payment or an authorized
19 agent of such covered entity, or, where applica-
20 ble, the service provider of such covered entity
21 acting with the express permission, and at the
22 direction of, that entity to assist with compli-
23 ance with the requirements of this subtitle.

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

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

4 “(H) The ransom payment instructions,
5 including information regarding where to send
6 the payment, such as the virtual currency ad-
7 dress or physical address the funds were re-
8 quested to be sent to, if applicable.

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

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

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

16 “(7) Deadlines for submitting reports to the Di-
17 rector required under subsection (a)(3), which
18 shall—

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

21 “(B) consider any existing regulatory re-
22 porting requirements similar in scope, purpose,
23 and timing to the reporting requirements to
24 which such a covered entity may also be sub-
25 ject, and make efforts to harmonize the timing

1 and contents of any such reports to the max-
2 imum extent practicable; and

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

6 “(8) Procedures for—

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

11 “(B) the Office to carry out the enforce-
12 ment provisions of section 2233, including with
13 respect to the issuance of subpoenas and other
14 aspects of noncompliance;

15 “(C) implementing the exceptions provided
16 in subparagraphs (A), (B), and (D) of sub-
17 section (a)(5); and

18 “(D) anonymizing and safeguarding infor-
19 mation received and disclosed through covered
20 cyber incident reports and ransom payment re-
21 ports that is known to be personal information
22 of a specific individual or information that iden-
23 tifies a specific individual that is not directly re-
24 lated to a cybersecurity threat.

1 “(d) THIRD-PARTY REPORT SUBMISSION AND RAN-
2 SOM PAYMENT.—

3 “(1) REPORT SUBMISSION.—An entity, includ-
4 ing a covered entity, that is required to submit a
5 covered cyber incident report or a ransom payment
6 report may use a third party, such as an incident re-
7 sponse company, insurance provider, service pro-
8 vider, information sharing and analysis organization,
9 or law firm, to submit the required report under
10 subsection (a).

11 “(2) RANSOM PAYMENT.—If an entity impacted
12 by a ransomware attack uses a third party to make
13 a ransom payment, the third party shall not be re-
14 quired to submit a ransom payment report for itself
15 under subsection (a)(2).

16 “(3) DUTY TO REPORT.—Third-party reporting
17 under this subparagraph does not relieve a covered
18 entity or an entity that makes a ransom payment
19 from the duty to comply with the requirements for
20 covered cyber incident report or ransom payment re-
21 port submission.

22 “(4) RESPONSIBILITY TO ADVISE.—Any third
23 party used by an entity that knowingly makes a ran-
24 som payment on behalf of an entity impacted by a
25 ransomware attack shall advise the impacted entity

1 of the responsibilities of the impacted entity regard-
2 ing a due diligence review under subsection (e) and
3 reporting ransom payments under this section.

4 “(e) DUE DILIGENCE REVIEW.—Before the date on
5 which a covered entity, or an entity that would be required
6 to submit a ransom payment report under this section if
7 that entity makes a ransom payment, makes a ransom
8 payment relating to a ransomware attack, the covered en-
9 tity or entity shall conduct a due diligence review of alter-
10 natives to making the ransom payment, including an anal-
11 ysis of whether the covered entity or entity can recover
12 from the ransomware attack through other means.

13 “(f) OUTREACH TO COVERED ENTITIES.—

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

22 “(2) ELEMENTS.—The outreach and education
23 campaign under paragraph (1) shall include the fol-
24 lowing:

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

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

7 “(C) An overview of the protections af-
8 farded to covered entities for complying with
9 the requirements under paragraphs (1), (2),
10 and (3) of subsection (a).

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

15 “(E) Specific outreach to cybersecurity
16 vendors, incident response providers, cybersecu-
17 rity insurance entities, and other entities that
18 may support covered entities or ransomware at-
19 tack victims.

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

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

1 “(A) the Critical Infrastructure Partner-
2 ship Advisory Council established under section
3 871;

4 “(B) information sharing and analysis or-
5 ganizations;

6 “(C) trade associations;

7 “(D) information sharing and analysis cen-
8 ters;

9 “(E) sector coordinating councils; and

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

12 “(g) EVALUATION OF STANDARDS.—

13 “(1) IN GENERAL.—Before issuing the final
14 rule pursuant to subsection (b)(2), the Director shall
15 review the data collected by the Office, and in con-
16 sultation with other appropriate entities, assess the
17 effectiveness of the rule with respect to—

18 “(A) the number of reports received;

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

20 “(C) the number of supplemental reports
21 required to be submitted; and

22 “(D) any other factor determined appro-
23 priate by the Director.

24 “(2) SUBMISSION TO CONGRESS.—The Director
25 shall submit to the Committee on Homeland Secu-

1 rity and Governmental Affairs of the Senate and the
2 Committee on Homeland Security of the House of
3 Representatives the results of the evaluation de-
4 scribed in paragraph (1) and may thereafter, in ac-
5 cordance with the requirements under subsection
6 (b), publish in the Federal Register a final rule im-
7 plementing this section.

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

15 **“SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER IN-**
16 **CIDENTS.**

17 “(a) IN GENERAL.—Entities may voluntarily report
18 incidents or ransom payments to the Director that are not
19 required under paragraph (1), (2), or (3) of section
20 2232(a), but may enhance the situational awareness of
21 cyber threats.

22 “(b) VOLUNTARY PROVISION OF ADDITIONAL INFOR-

23 MATION IN REQUIRED REPORTS.—Entities may volun-

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

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

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

3 “(e) APPLICATION OF PROTECTIONS.—The protec-
4 tions under section 2235 applicable to covered cyber inci-
5 dent reports shall apply in the same manner and to the
6 same extent to reports and information submitted under
7 subsections (a) and (b).

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

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

21 “(b) INITIAL REQUEST FOR INFORMATION.—

22 “(1) IN GENERAL.—If the Director has reason
23 to believe, whether through public reporting or other
24 information in the possession of the Federal Govern-
25 ment, including through analysis performed pursu-

1 ant to paragraph (1) or (2) of section 2231(b), that
2 an entity has experienced a covered cyber incident or
3 made a ransom payment but failed to report such
4 incident or payment to the Office within 72 hours in
5 accordance to section 2232(a), the Director shall re-
6 quest additional information from the entity to con-
7 firm whether or not a covered cyber incident or ran-
8 som payment has occurred.

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

13 “(c) AUTHORITY TO ISSUE SUBPOENAS AND
14 DEBAR.—

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

25 “(2) CIVIL ACTION.—

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

6 “(B) VENUE.—An action under this para-
7 graph may be brought in the judicial district in
8 which the entity against which the action is
9 brought resides, is found, or does business.

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

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

17 “(4) DEBARMENT OF FEDERAL CONTRAC-
18 TORS.—If a covered entity with a Federal Govern-
19 ment contract, grant, or cooperative agreement fails
20 to comply with a subpoena issued under this sub-
21 section—

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

24 “(B) upon receiving a referral from the Di-
25 rector, the Administrator of General Services

1 may impose additional available penalties, in-
2 cluding suspension or debarment.

3 “(d) PROVISION OF CERTAIN INFORMATION TO AT-
4 TORNEY GENERAL.—

5 “(1) IN GENERAL.—Notwithstanding section
6 2235(a) and subsection (b)(2) of this section, if the
7 Director determines, based on the information pro-
8 vided in response to the subpoena issued pursuant to
9 subsection (c), that the facts relating to the covered
10 cyber incident or ransom payment at issue may con-
11 stitute grounds for a regulatory enforcement action
12 or criminal prosecution, the Director may provide
13 that information to the Attorney General or the ap-
14 propriate regulator, who may use that information
15 for a regulatory enforcement action or criminal pros-
16 ecution.

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

1 “(3) **RULE OF CONSTRUCTION.**—Nothing in
2 this subtitle shall be construed to provide an entity
3 that submits a covered cyber incident report or ran-
4 som payment report under section ~~2232~~ any immu-
5 nity from law enforcement action for making a ran-
6 som payment otherwise prohibited by law.

7 “(e) **CONSIDERATIONS.**—When determining whether
8 to exercise the authorities provided under this section, the
9 Director shall take into consideration—

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

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

13 “(3) prior interaction with the Agency or
14 awareness of the entity of the policies and proce-
15 dures of the Agency for reporting covered cyber inci-
16 dents and ransom payments; and

17 “(4) for non-covered entities required to submit
18 a ransom payment report, the ability of the entity to
19 perform a due diligence review pursuant to section
20 ~~2232~~(e).

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

23 “(g) **REPORT TO CONGRESS.**—The Director shall
24 submit to Congress an annual report on the number of
25 times the Director—

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

3 “(2) issued a subpoena pursuant to subsection
4 (c);

5 “(3) brought a civil action pursuant to sub-
6 section (e)(2); or

7 “(4) conducted additional actions pursuant to
8 subsection (d).

9 **“SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO**
10 **THE FEDERAL GOVERNMENT.**

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

12 “(1) AUTHORIZED ACTIVITIES.—Information
13 provided to the Office or Agency pursuant to section
14 2232 may be disclosed to, retained by, and used by,
15 consistent with otherwise applicable provisions of
16 Federal law, any Federal agency or department,
17 component, officer, employee, or agent of the Fed-
18 eral Government solely for—

19 “(A) a cybersecurity purpose;

20 “(B) the purpose of identifying—

21 “(i) a cyber threat, including the
22 source of the cyber threat; or

23 “(ii) a security vulnerability;

24 “(C) the purpose of responding to, or oth-
25 erwise preventing or mitigating, a specific

1 threat of death, a specific threat of serious bod-
2 ily harm, or a specific threat of serious eco-
3 nomic harm, including a terrorist act or a use
4 of a weapon of mass destruction;

5 “(D) the purpose of responding to, inves-
6 tigating, prosecuting, or otherwise preventing or
7 mitigating, a serious threat to a minor, includ-
8 ing sexual exploitation and threats to physical
9 safety; or

10 “(E) the purpose of preventing, inves-
11 tigating, disrupting, or prosecuting an offense
12 arising out of a covered cyber incident or any
13 of the offenses listed in section 105(d)(5)(A)(v)
14 of the Cybersecurity Act of 2015 (6 U.S.C.
15 1504(d)(5)(A)(v)).

16 “(2) AGENCY ACTIONS AFTER RECEIPT.—

17 “(A) RAPID, CONFIDENTIAL SHARING OF
18 CYBER THREAT INDICATORS.—Upon receiving a
19 covered cyber incident or ransom payment re-
20 port submitted pursuant to this section, the Of-
21 fice shall immediately review the report to de-
22 termine whether the incident that is the subject
23 of the report is connected to an ongoing cyber
24 threat or security vulnerability and where appli-
25 cable, use such report to identify, develop, and

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

4 “(B) STANDARDS FOR SHARING SECURITY
5 VULNERABILITIES.—With respect to informa-
6 tion in a covered cyber incident or ransom pay-
7 ment report regarding a security vulnerability
8 referred to in paragraph (1)(B)(ii), the Director
9 shall develop principles that govern the timing
10 and manner in which information relating to se-
11 curity vulnerabilities may be shared, consistent
12 with common industry best practices and
13 United States and international standards.

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

1 “(A) personal information of a specific in-
2 dividual; or

3 “(B) information that identifies a specific
4 individual that is not directly related to a cyber-
5 security threat.

6 “(4) DIGITAL SECURITY.—The Office shall en-
7 sure that reports submitted to the Office pursuant
8 to section 2232, and any information contained in
9 those reports, are collected, stored, and protected at
10 a minimum in accordance with the requirements for
11 moderate impact Federal information systems, as
12 described in Federal Information Processing Stand-
13 ards Publication 199, or any successor document.

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

22 “(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—
23 The submission of a report under section 2232 to the Of-
24 fice shall not constitute a waiver of any applicable privilege

1 or protection provided by law, including trade secret pro-
2 tection and attorney-client privilege.

3 “(e) EXEMPTION FROM DISCLOSURE.—Information
4 contained in a report submitted to the Office under section
5 2232 shall be exempt from disclosure under section
6 552(b)(3)(B) of title 5, United States Code (commonly
7 known as the ‘Freedom of Information Act’) and any
8 State, Tribal, or local provision of law requiring disclosure
9 of information or records.

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

15 “(e) LIABILITY PROTECTIONS.—

16 “(1) IN GENERAL.—No cause of action shall lie
17 or be maintained in any court by any person or enti-
18 ty and any such action shall be promptly dismissed
19 for the submission of a report pursuant to section
20 2232(a) that is submitted in conformance with this
21 subtitle and the rules promulgated under section
22 2232(b), except that this subsection shall not apply
23 with regard to an action by the Federal Government
24 pursuant to section 2234(e)(2).

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

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

16 “(g) PROPRIETARY INFORMATION.—Information
 17 contained in a report submitted to the Agency under section
 18 2232 shall be considered the commercial, financial,
 19 and proprietary information of the covered entity when so
 20 designated by the covered entity.”.

21 “(c) TECHNICAL AND CONFORMING AMENDMENT.—
 22 The table of contents in section 1(b) of the Homeland Security
 23 Act of 2002 (Public Law 107–296; 116 Stat. 2135)
 24 is amended by inserting after the items relating to subtitle
 25 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.”.

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

2 (a) **CYBER INCIDENT REPORTING SHARING.**—Not-
 3 withstanding any other provision of law or regulation, any
 4 Federal agency that receives a report from an entity of
 5 a cyber attack, including a ransomware attack, shall pro-
 6 vide all such information to the Director of the Cybersecu-
 7 rity Infrastructure Security Agency not later than 24
 8 hours after receiving the report, unless a shorter period
 9 is required by an agreement made between the Cyber Inci-
 10 dent Review Office established under section 2231 of the
 11 Homeland Security Act of 2002, as added by section 3(b)
 12 of this Act, and another Federal entity.

13 (b) **CREATION OF COUNCIL.**—Section 1752(c)(1) of
 14 the William M. (Mac) Thornberry National Defense Au-
 15 thorization Act for Fiscal Year 2021 (6 U.S.C.
 16 1500(c)(1)) is amended—

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

19 (2) by redesignating subparagraph (H) as sub-
 20 paragraph (I); and

21 (3) by inserting after subparagraph (G) the fol-
 22 lowing:

1 “(H) lead an intergovernmental Cyber In-
2 cident Reporting Council, in coordination with
3 the Director of the Office of Management and
4 Budget and the Director of the Cybersecurity
5 and Infrastructure Security Agency and in con-
6 sultation with Sector Risk Management Agen-
7 cies (as defined in section 2201 of the Home-
8 land Security Act of 2002 (6 U.S.C. 651)) and
9 other appropriate Federal agencies, to coordi-
10 nate, deconflict, and harmonize Federal incident
11 reporting requirements, including those issued
12 through regulations, for covered entities (as de-
13 fined in section 2230 of such Act) and entities
14 that make a ransom payment (as defined in
15 such section 2201 (6 U.S.C. 651)); and”.

16 (e) HARMONIZING REPORTING REQUIREMENTS.—
17 The National Cyber Director shall, in consultation with
18 the Director, the Cyber Incident Reporting Council de-
19 scribed in section 1752(e)(1)(H) of the William M. (Mac)
20 Thornberry National Defense Authorization Act for Fiscal
21 Year 2021 (6 U.S.C. 1500(e)(1)(H)), and the Director of
22 the Office of Management and Budget, to the maximum
23 extent practicable—

24 (1) review existing regulatory requirements, in-
25 cluding the information required in such reports, to

1 report cyber incidents and ensure that any such re-
2 porting requirements and procedures avoid con-
3 flicting, duplicative, or burdensome requirements;
4 and

5 (2) coordinate with the Director and regulatory
6 authorities that receive reports relating to cyber inci-
7 dents to identify opportunities to streamline report-
8 ing processes, and where feasible, facilitate inter-
9 agency agreements between such authorities to per-
10 mit the sharing of such reports, consistent with ap-
11 plicable law and policy, without impacting the ability
12 of such agencies to gain timely situational awareness
13 of a covered cyber incident or ransom payment.

14 **SEC. 5. RANSOMWARE VULNERABILITY WARNING PILOT**
15 **PROGRAM.**

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

1 (b) IDENTIFICATION OF VULNERABLE SYSTEMS.—

2 The pilot program established under subsection (a) shall—

3 (1) identify the most common security vulnera-
4 bilities utilized in ransomware attacks and mitiga-
5 tion techniques; and

6 (2) utilize existing authorities to identify Fed-
7 eral and other relevant information systems that
8 contain the security vulnerabilities identified in para-
9 graph (1).

10 (c) ENTITY NOTIFICATION.—

11 (1) IDENTIFICATION.—If the Director is able to
12 identify the entity at risk that owns or operates a
13 vulnerable information system identified in sub-
14 section (b), the Director may notify the owner of the
15 information system.

16 (2) NO IDENTIFICATION.—If the Director is not
17 able to identify the entity at risk that owns or oper-
18 ates a vulnerable information system identified in
19 subsection (b), the Director may utilize the subpoena
20 authority pursuant to section 2209 of the Homeland
21 Security Act of 2002 (6 U.S.C. 659) to identify and
22 notify the entity at risk pursuant to the procedures
23 within that section.

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

1 on the identified security vulnerability and mitiga-
2 tion techniques.

3 (d) **PRIORITIZATION OF NOTIFICATIONS.**—To the ex-
4 tent practical, the Director shall prioritize covered entities
5 for identification and notification activities under the pilot
6 program established under this section.

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

13 (f) **RULE OF CONSTRUCTION.**—Nothing in this sec-
14 tion shall be construed to provide additional authorities
15 to the Director to identify vulnerabilities or vulnerable sys-
16 tems.

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

18 (a) **JOINT RANSOMWARE TASK FORCE.**—

19 (1) **IN GENERAL.**—Not later than 180 days
20 after the date of enactment of this section, the Na-
21 tional Cyber Director shall establish and chair the
22 Joint Ransomware Task Force to coordinate an on-
23 going, nationwide campaign against ransomware at-
24 tacks, and identify and pursue opportunities for
25 international cooperation.

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

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

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

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

17 (C) Identifying, in consultation with rel-
18 evant entities, a list of highest threat ransom-
19 ware entities updated on an ongoing basis, in
20 order to facilitate—

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

23 (ii) identify metrics for success of said
24 actions.

1 (D) Disrupting ransomware criminal ac-
2 tors, associated infrastructure, and their fi-
3 nances.

4 (E) Facilitating coordination and collabo-
5 ration between Federal entities and relevant en-
6 tities, including the private sector, to improve
7 Federal actions against ransomware threats.

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

10 (G) Creation of after-action reports and
11 other lessons learned from Federal actions that
12 identify successes and failures to improve sub-
13 sequent actions.

14 (H) Any other activities determined appro-
15 priate by the task force to mitigate the threat
16 of ransomware attacks against Federal and
17 non-Federal entities.

18 (b) ~~CLARIFYING PRIVATE-SECTOR LAWFUL DEFEN-~~
19 ~~SIVE MEASURES.~~—Not later than 180 days after the date
20 of enactment of this Act, the National Cyber Director, in
21 coordination with the Secretary of Homeland Security and
22 the Attorney General, shall submit to the Committee on
23 Homeland Security and Governmental Affairs and the
24 Committee on the Judiciary of the Senate and the Com-
25 mittee on Homeland Security, the Committee on the Judi-

1 ciary, and the Committee on Oversight and Reform of the
2 House of Representatives a report that describes defensive
3 measures that private-sector actors can take when coun-
4 tering ransomware attacks and what laws need to be clari-
5 fied to enable that action.

6 (c) **RULE OF CONSTRUCTION.**—Nothing in this sec-
7 tion shall be construed as providing any additional author-
8 ity to any Federal agency.

9 **SEC. 7. CONGRESSIONAL REPORTING.**

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

20 (b) **REPORT ON OPPORTUNITIES TO STRENGTHEN**
21 **SECURITY RESEARCH.**—Not later than 1 year after the
22 date of enactment of this Act, the Director shall submit
23 to the Committee on Homeland Security and Govern-
24 mental Affairs of the Senate and the Committee on Home-
25 land Security of the House of Representatives a report de-

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

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

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

20 (2) The identification of most common vulnera-
21 bilities utilized in ransomware.

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

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

4 (d) ~~REPORT ON HARMONIZATION OF REPORTING~~
5 ~~REGULATIONS.~~—Not later than 180 days after the date
6 on which the National Cyber Director convenes the Coun-
7 cil described in section 1752(c)(1)(H) of the William M.
8 (Mac) Thornberry National Defense Authorization Act for
9 Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National
10 Cyber Director shall submit to the appropriate congres-
11 sional committees a report that includes—

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

15 (2) any actions the National Cyber Director in-
16 tends to take to harmonize the duplicative reporting
17 requirements; and

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

20 (e) ~~GAO REPORT.~~—Not later than 2 years after the
21 date of enactment of this Act, the Comptroller General
22 of the United States shall submit to the Committee on
23 Homeland Security and Governmental Affairs of the Sen-
24 ate and the Committee on Homeland Security of the

1 House of Representatives a report on the implementation
2 of this Act and the amendments made by this Act.

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:*

8 (1) *COVERED CYBER INCIDENT; COVERED ENTI-*
9 *TY; CYBER INCIDENT.—The terms “covered cyber inci-*
10 *dent”, “covered entity”, and “cyber incident” have*
11 *the meanings given those terms in section 2230 of the*
12 *Homeland Security Act of 2002, as added by section*
13 *3(b) of this Act.*

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

20 (3) *DIRECTOR.—The term “Director” means the*
21 *Director of the Cybersecurity and Infrastructure Se-*
22 *curity Agency.*

23 (4) *INFORMATION SYSTEM; SECURITY VULNER-*
24 *ABILITY.—The terms “information system” and “se-*
25 *curity vulnerability” have the meanings given those*

1 *terms in section 102 of the Cybersecurity Act of 2015*
2 *(6 U.S.C. 1501).*

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

4 *(a) DEFINITIONS.—*

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

7 *(A) by redesignating paragraphs (1), (2),*
8 *(3), (4), (5), and (6) as paragraphs (2), (4), (5),*
9 *(7), (10), and (11), respectively;*

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

12 *“(1) CLOUD SERVICE PROVIDER.—The term*
13 *‘cloud service provider’ means an entity offering*
14 *products or services related to cloud computing, as de-*
15 *defined by the National Institutes of Standards and*
16 *Technology in NIST Special Publication 800–145*
17 *and any amendatory or superseding document relat-*
18 *ing thereto.”;*

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

21 *“(3) CYBER ATTACK.—The term ‘cyber attack’*
22 *means the use of unauthorized or malicious code on*
23 *an information system, or the use of another digital*
24 *mechanism such as a denial of service attack, to in-*
25 *terrupt or disrupt the operations of an information*

1 *system or compromise the confidentiality, avail-*
2 *ability, or integrity of electronic data stored on, proc-*
3 *essed by, or transiting an information system.”;*

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

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

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

15 *“(8) RANSOM PAYMENT.—The term ‘ransom pay-*
16 *ment’ means the transmission of any money or other*
17 *property or asset, including virtual currency, or any*
18 *portion thereof, which has at any time been delivered*
19 *as ransom in connection with a ransomware attack.*

20 *“(9) RANSOMWARE ATTACK.—The term*
21 *‘ransomware attack’—*

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

1 *service attack, to interrupt or disrupt the oper-*
2 *ations of an information system or compromise*
3 *the confidentiality, availability, or integrity of*
4 *electronic data stored on, processed by, or*
5 *transiting an information system to extort a de-*
6 *mand for a ransom payment; and*

7 *“(B) does not include any such event where*
8 *the demand for payment is made by a Federal*
9 *Government entity, good-faith security research,*
10 *or in response to an invitation by the owner or*
11 *operator of the information system for third par-*
12 *ties to identify vulnerabilities in the information*
13 *system.”; and*

14 *(F) by adding at the end the following:*

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

23 *“(14) VIRTUAL CURRENCY.—The term ‘virtual*
24 *currency’ means the digital representation of value*

1 *that functions as a medium of exchange, a unit of ac-*
 2 *count, or a store of value.*

3 “(15) *VIRTUAL CURRENCY ADDRESS.*—*The term*
 4 *‘virtual currency address’ means a unique public*
 5 *cryptographic key identifying the location to which a*
 6 *virtual currency payment can be made.”.*

7 (2) *CONFORMING AMENDMENT.*—*Section*
 8 *9002(A)(7) of the William M. (Mac) Thornberry Na-*
 9 *tional Defense Authorization Act for Fiscal Year 2021*
 10 *(6 U.S.C. 652a(a)(7)) is amended to read as follows:*

11 “(7) *SECTOR RISK MANAGEMENT AGENCY.*—*The*
 12 *term ‘Sector Risk Management Agency’ has the mean-*
 13 *ing given the term in section 2201 of the Homeland*
 14 *Security Act of 2002 (6 U.S.C. 651).”.*

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

18 **“Subtitle C—Cyber Incident**
 19 **Reporting**

20 **“SEC. 2230. DEFINITIONS.**

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

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

1 “(1) *COUNCIL.*—*The term ‘Council’ means the*
2 *Cyber Incident Reporting Council described in section*
3 *1752(c)(1)(H) of the William M. (Mac) Thornberry*
4 *National Defense Authorization Act for Fiscal Year*
5 *2021 (6 U.S.C. 1500(c)(1)(H)).*

6 “(2) *COVERED CYBER INCIDENT.*—*The term ‘cov-*
7 *ered cyber incident’ means a substantial cyber inci-*
8 *dent experienced by a covered entity that satisfies the*
9 *definition and criteria established by the Director in*
10 *the interim final rule and final rule issued pursuant*
11 *to section 2232.*

12 “(3) *COVERED ENTITY.*—*The term ‘covered enti-*
13 *ty’ means an entity that owns or operates critical in-*
14 *frastructure that satisfies the definition established by*
15 *the Director in the interim final rule and final rule*
16 *issued pursuant to section 2232.*

17 “(4) *CYBER INCIDENT.*—*The term ‘cyber inci-*
18 *dent’ has the meaning given the term ‘incident’ in*
19 *section 2209(a).*

20 “(5) *CYBER THREAT.*—*The term ‘cyber threat’—*

21 *“(A) has the meaning given the term ‘cyber-*
22 *security threat’ in section 102 of the Cybersecu-*
23 *rity Act of 2015 (6 U.S.C. 1501); and*

24 *“(B) does not include any activity related*
25 *to good faith security research, including partici-*

1 *pation in a bug-bounty program or a vulner-*
2 *ability disclosure program.*

3 “(6) *CYBER THREAT INDICATOR; CYBERSECURITY*
4 *PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY;*
5 *INFORMATION SYSTEM; SECURITY CONTROL; SECURITY*
6 *VULNERABILITY.—The terms ‘cyber threat indicator’,*
7 *‘cybersecurity purpose’, ‘defensive measure’, ‘Federal*
8 *entity’, ‘information system’, ‘security control’, and*
9 *‘security vulnerability’ have the meanings given those*
10 *terms in section 102 of the Cybersecurity Act of 2015*
11 *(6 U.S.C. 1501).*

12 “(7) *SMALL ORGANIZATION.—The term ‘small or-*
13 *ganization’—*

14 “(A) *means—*

15 “(i) *a small business concern, as de-*
16 *defined in section 3 of the Small Business Act*
17 *(15 U.S.C. 632); or*

18 “(ii) *any business, nonprofit organiza-*
19 *tion, or other private sector entity with*
20 *fewer than 50 employees (determined on a*
21 *full-time equivalent basis); and*

22 “(B) *does not include—*

23 “(i) *a business, nonprofit organization,*
24 *or other private sector entity that is a cov-*
25 *ered entity; or*

1 “(ii) a business, nonprofit organiza-
 2 tion, or other private sector entity that
 3 holds a government contract, unless that
 4 contractor is a party only to—

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

7 “(II) a contract to provide prod-
 8 ucts or services unrelated to informa-
 9 tion technology that is below the micro-
 10 purchase threshold, as defined in sec-
 11 tion 2.101 of title 48, Code of Federal
 12 Regulations, or any successor regula-
 13 tion.

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

15 “(a) *CYBER INCIDENT REVIEW OFFICE.*—There is es-
 16 tablished in the Agency a Cyber Incident Review Office (in
 17 this section referred to as the ‘Office’) to receive, aggregate,
 18 and analyze reports related to covered cyber incidents sub-
 19 mitted by covered entities and reports related to ransom
 20 payments submitted by entities in furtherance of the activi-
 21 ties specified in subsection (b) of this section and sections
 22 2202(e), 2203, and 2209(c) and any other authorized activ-
 23 ity of the Director to enhance the situational awareness of
 24 cyber threats across critical infrastructure sectors.

1 “(b) *ACTIVITIES.*—*The Office shall, in furtherance of*
2 *the activities specified in sections 2202(e), 2203, and*
3 *2209(c)—*

4 “(1) *receive, aggregate, analyze, and secure, con-*
5 *sistent with the requirements under the Cybersecurity*
6 *Information Sharing Act of 2015 (6 U.S.C. 1501 et*
7 *seq.) reports from covered entities related to a covered*
8 *cyber incident to assess the effectiveness of security*
9 *controls and identify tactics, techniques, and proce-*
10 *dures adversaries use to overcome those controls;*

11 “(2) *receive, aggregate, analyze, and secure re-*
12 *ports related to ransom payments to identify tactics,*
13 *techniques, and procedures, including identifying and*
14 *tracking ransom payments utilizing virtual cur-*
15 *rencies, adversaries use to perpetuate ransomware at-*
16 *tacks and facilitate ransom payments;*

17 “(3) *leverage information gathered about cyberse-*
18 *curity incidents to—*

19 “(A) *enhance the quality and effectiveness of*
20 *information sharing and coordination efforts*
21 *with appropriate entities, including agencies,*
22 *sector coordinating councils, information sharing*
23 *and analysis organizations, technology providers,*
24 *cybersecurity and incident response firms, and*
25 *security researchers; and*

1 “(B) provide appropriate entities, including
2 agencies, sector coordinating councils, informa-
3 tion sharing and analysis organizations, tech-
4 nology providers, cybersecurity and incident re-
5 sponse firms, and security researchers, with
6 timely, actionable, and anonymized reports of
7 cyber attack campaigns and trends, including, to
8 the maximum extent practicable, related contex-
9 tual information, cyber threat indicators, and
10 defensive measures;

11 “(4) establish mechanisms to receive feedback
12 from stakeholders on how the Agency can most effec-
13 tively receive covered cyber incident reports, ransom
14 payment reports, and other voluntarily provided in-
15 formation;

16 “(5) facilitate the timely sharing, on a voluntary
17 basis, between relevant critical infrastructure owners
18 and operators of information relating to covered cyber
19 incidents and ransom payments, particularly with re-
20 spect to ongoing cyber threats or security
21 vulnerabilities and identify and disseminate ways to
22 prevent or mitigate similar incidents in the future;

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

1 *of related cyber incidents that together satisfy such*
2 *definition, conduct a review of the details sur-*
3 *rounding the covered cyber incident or group of those*
4 *incidents and identify and disseminate ways to pre-*
5 *vent or mitigate similar incidents in the future;*

6 *“(7) with respect to covered cyber incident re-*
7 *ports under subsection (c) involving an ongoing cyber*
8 *threat or security vulnerability, immediately review*
9 *those reports for cyber threat indicators that can be*
10 *anonymized and disseminated, with defensive meas-*
11 *ures, to appropriate stakeholders, in coordination*
12 *with other divisions within the Agency, as appro-*
13 *priate;*

14 *“(8) publish quarterly unclassified, public re-*
15 *ports that may be based on the unclassified informa-*
16 *tion contained in the reports required under sub-*
17 *section (c);*

18 *“(9) proactively identify opportunities and per-*
19 *form analyses, consistent with the protections in sec-*
20 *tion 2235, to leverage and utilize data on ransom at-*
21 *tacks to support law enforcement operations to iden-*
22 *tify, track, and seize ransom payments utilizing vir-*
23 *tual currencies, to the greatest extent practicable;*

24 *“(10) proactively identify opportunities, con-*
25 *sistent with the protections in section 2235, to lever-*

1 *age and utilize data on cyber incidents in a manner*
2 *that enables and strengthens cybersecurity research*
3 *carried out by academic institutions and other pri-*
4 *rate sector organizations, to the greatest extent prac-*
5 *ticable;*

6 *“(11) on a not less frequently than annual basis,*
7 *analyze public disclosures made pursuant to parts*
8 *229 and 249 of title 17, Code of Federal Regulations,*
9 *or any subsequent document submitted to the Securi-*
10 *ties and Exchange Commission by entities experi-*
11 *encing cyber incidents and compare such disclosures*
12 *to reports received by the Office; and*

13 *“(12) in accordance with section 2235, not later*
14 *than 24 hours after receiving a covered cyber incident*
15 *report or ransom payment report, share the reported*
16 *information with appropriate Sector Risk Manage-*
17 *ment Agencies and other appropriate agencies as de-*
18 *termined by the Director of Office Management and*
19 *Budget, in consultation with the Director and the Na-*
20 *tional Cyber Director.*

21 *“(c) PERIODIC REPORTING.—Not later than 60 days*
22 *after the effective date of the interim final rule required*
23 *under section 2232(b)(1), and on the first day of each*
24 *month thereafter, the Director, in consultation with the At-*
25 *torney General and the Director of National Intelligence,*

1 *shall submit to the National Cyber Director, the majority*
2 *leader of the Senate, the minority leader of the Senate, the*
3 *Speaker of the House of Representatives, the minority lead-*
4 *er of the House of Representatives, the Committee on Home-*
5 *land Security and Governmental Affairs of the Senate, and*
6 *the Committee on Homeland Security of the House of Rep-*
7 *resentatives a report that characterizes the national cyber*
8 *threat landscape, including the threat facing Federal agen-*
9 *cies and covered entities and applicable intelligence and*
10 *law enforcement information, covered cyber incidents, and*
11 *ransomware attacks, as of the date of the report, which*
12 *shall—*

13 “(1) *include the total number of reports sub-*
14 *mitted under sections 2232 and 2233 during the pre-*
15 *ceding month, including a breakdown of required and*
16 *voluntary reports;*

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

23 “(A) *the infrastructure, tactics, and tech-*
24 *niques malicious cyber actors commonly use; and*

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

4 *“(3) SUPPLEMENTAL REPORTS.—A covered enti-*
5 *ty shall promptly submit to the Director an update*
6 *or supplement to a previously submitted covered cyber*
7 *incident report if new or different information be-*
8 *comes available or if the covered entity makes a ran-*
9 *som payment after submitting a covered cyber inci-*
10 *dent report required under paragraph (1).*

11 *“(4) PRESERVATION OF INFORMATION.—Any en-*
12 *tity subject to requirements of paragraph (1), (2), or*
13 *(3) shall preserve data relevant to the covered cyber*
14 *incident or ransom payment in accordance with pro-*
15 *cedures established in the interim final rule and final*
16 *rule issued pursuant to subsection (b).*

17 *“(5) EXCEPTIONS.—*

18 *“(A) REPORTING OF COVERED CYBER INCI-*
19 *DENT WITH RANSOM PAYMENT.—If a covered*
20 *cyber incident includes a ransom payment such*
21 *that the reporting requirements under para-*
22 *graphs (1) and (2) apply, the covered entity may*
23 *submit a single report to satisfy the requirements*
24 *of both paragraphs in accordance with proce-*

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

3 “(B) *SUBSTANTIALLY SIMILAR REPORTED*
4 *INFORMATION.—The requirements under para-*
5 *graphs (1), (2), and (3) shall not apply to an en-*
6 *tity required by law, regulation, or contract to*
7 *report substantially similar information to an-*
8 *other Federal agency within a substantially*
9 *similar timeframe.*

10 “(6) *MANNER, TIMING, AND FORM OF RE-*
11 *PORTS.—Reports made under paragraphs (1), (2),*
12 *and (3) shall be made in the manner and form, and*
13 *within the time period in the case of reports made*
14 *under paragraph (3), prescribed according to the in-*
15 *terim final rule and final rule issued pursuant to*
16 *subsection (b).*

17 “(7) *EFFECTIVE DATE.—Paragraphs (1) through*
18 *(4) shall take effect on the dates prescribed in the in-*
19 *terim final rule and the final rule issued pursuant to*
20 *subsection (b), except that the requirements of para-*
21 *graphs (1) through (4) shall not be effective for a pe-*
22 *riod for more than 18 months after the effective date*
23 *of the interim final rule if the Director has not issued*
24 *a final rule pursuant to subsection (b)(2).*

25 “(b) *RULEMAKING.—*

1 “(1) *INTERIM FINAL RULE.*—Not later than 270
2 *days after the date of enactment of this section, and*
3 *after a 60-day consultative period, followed by a 90-*
4 *day comment period with appropriate stakeholders,*
5 *the Director, in consultation with Sector Risk Man-*
6 *agement Agencies and the heads of other Federal*
7 *agencies, shall publish in the Federal Register an in-*
8 *terim final rule to implement subsection (a).*

9 “(2) *FINAL RULE.*—Not later than 1 year after
10 *publication of the interim final rule under paragraph*
11 *(1), the Director shall publish a final rule to imple-*
12 *ment subsection (a).*

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

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

24 “(1) *A clear description of the types of entities*
25 *that constitute covered entities, based on—*

1 “(A) *the consequences that disruption to or*
2 *compromise of such an entity could cause to na-*
3 *tional security, economic security, or public*
4 *health and safety;*

5 “(B) *the likelihood that such an entity may*
6 *be targeted by a malicious cyber actor, including*
7 *a foreign country; and*

8 “(C) *the extent to which damage, disrup-*
9 *tion, or unauthorized access to such an entity,*
10 *including the accessing of sensitive cybersecurity*
11 *vulnerability information or penetration testing*
12 *tools or techniques, will likely enable the disrup-*
13 *tion of the reliable operation of critical infra-*
14 *structure.*

15 “(2) *A clear description of the types of substan-*
16 *tial cyber incidents that constitute covered cyber inci-*
17 *dents, which shall—*

18 “(A) *at a minimum, require the occurrence*
19 *of—*

20 “(i) *the unauthorized access to an in-*
21 *formation system or network with a sub-*
22 *stantial loss of confidentiality, integrity, or*
23 *availability of such information system or*
24 *network, or a serious impact on the safety*

1 *and resiliency of operational systems and*
2 *processes;*

3 *“(ii) a disruption of business or indus-*
4 *trial operations due to a cyber incident; or*

5 *“(iii) an occurrence described in clause*
6 *(i) or (ii) due to loss of service facilitated*
7 *through, or caused by, a compromise of a*
8 *cloud service provider, managed service pro-*
9 *vider, or other third-party data hosting pro-*
10 *vider or by a supply chain compromise;*

11 *“(B) consider—*

12 *“(i) the sophistication or novelty of the*
13 *tactics used to perpetrate such an incident,*
14 *as well as the type, volume, and sensitivity*
15 *of the data at issue;*

16 *“(ii) the number of individuals di-*
17 *rectly or indirectly affected or potentially*
18 *affected by such an incident; and*

19 *“(iii) potential impacts on industrial*
20 *control systems, such as supervisory control*
21 *and data acquisition systems, distributed*
22 *control systems, and programmable logic*
23 *controllers; and*

24 *“(C) exclude—*

1 “(i) any event where the cyber incident
2 is perpetuated by a United States Govern-
3 ment entity, good-faith security research, or
4 in response to an invitation by the owner or
5 operator of the information system for third
6 parties to find vulnerabilities in the infor-
7 mation system, such as a through a vulner-
8 ability disclosure program or the use of au-
9 thorized penetration testing services; and

10 “(ii) the threat of disruption as extor-
11 tion, as described in section 2201(9)(A).

12 “(3) A requirement that, if a covered cyber inci-
13 dent or a ransom payment occurs following an ex-
14 empted threat described in paragraph (2)(C)(ii), the
15 entity shall comply with the requirements in this sub-
16 title in reporting the covered cyber incident or ran-
17 som payment.

18 “(4) A clear description of the specific required
19 contents of a report pursuant to subsection (a)(1),
20 which shall include the following information, to the
21 extent applicable and available, with respect to a cov-
22 ered cyber incident:

23 “(A) A description of the covered cyber inci-
24 dent, including—

1 “(i) identification and a description of
2 the function of the affected information sys-
3 tems, networks, or devices that were, or are
4 reasonably believed to have been, affected by
5 such incident;

6 “(ii) a description of the unauthorized
7 access with substantial loss of confiden-
8 tiality, integrity, or availability of the af-
9 fected information system or network or dis-
10 ruption of business or industrial operations;

11 “(iii) the estimated date range of such
12 incident; and

13 “(iv) the impact to the operations of
14 the covered entity.

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

19 “(C) Where applicable, any identifying or
20 contact information related to each actor reason-
21 ably believed to be responsible for such incident.

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

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 telephone
6 number or electronic mail address, that the Of-
7 fice may use to contact the covered entity or an
8 authorized agent of such covered entity, or, where
9 applicable, the service provider of such covered
10 entity acting with the express permission, and at
11 the direction, of the covered entity to assist with
12 compliance with the requirements of this subtitle.

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

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

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

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

1 *reasonably believed to be responsible for the*
2 *ransomware attack.*

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

6 “(E) *Contact information, such as telephone*
7 *number or electronic mail address, that the Of-*
8 *fice may use to contact the entity that made the*
9 *ransom payment or an authorized agent of such*
10 *covered entity, or, where applicable, the service*
11 *provider of such covered entity acting with the*
12 *express permission, and at the direction of, that*
13 *entity to assist with compliance with the require-*
14 *ments of this subtitle.*

15 “(F) *The date of the ransom payment.*

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

19 “(H) *The ransom payment instructions, in-*
20 *cluding information regarding where to send the*
21 *payment, such as the virtual currency address or*
22 *physical address the funds were requested to be*
23 *sent to, if applicable.*

24 “(I) *The amount of the ransom payment.*

1 “(J) A summary of the due diligence review
2 required under subsection (e).

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

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

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

11 “(B) consider any existing regulatory re-
12 porting requirements similar in scope, purpose,
13 and timing to the reporting requirements to
14 which such a covered entity may also be subject,
15 and make efforts to harmonize the timing and
16 contents of any such reports to the maximum ex-
17 tent practicable; and

18 “(C) balance the need for situational aware-
19 ness with the ability of the covered entity to con-
20 duct incident response and investigations.

21 “(8) Procedures for—

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

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

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

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

15 “(9) A clear description of the types of entities
16 that constitute other private sector entities for pur-
17 poses of section 2230(b)(7).

18 “(d) *THIRD PARTY REPORT SUBMISSION AND RANSOM*
19 *PAYMENT.*—

20 “(1) *REPORT SUBMISSION.*—An entity, including
21 a covered entity, that is required to submit a covered
22 cyber incident report or a ransom payment report
23 may use a third party, such as an incident response
24 company, insurance provider, service provider, infor-
25 mation sharing and analysis organization, or law

1 *firm, to submit the required report under subsection*
2 *(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 of*
18 *the responsibilities of the impacted entity regarding a*
19 *due diligence review under subsection (e) and report-*
20 *ing 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 pay-*
25 *ment relating to a ransomware attack, the covered entity*

1 *or entity shall conduct a due diligence review of alternatives*
2 *to making the ransom payment, including an analysis of*
3 *whether the covered entity or entity can recover from the*
4 *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 pay-*
10 *ments on behalf of entities impacted by ransomware*
11 *attacks, potential ransomware attack victims, and*
12 *other appropriate entities of the requirements of para-*
13 *graphs (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 afforded*
24 *to covered entities for complying with the re-*

1 *quirements under paragraphs (1), (2), and (3) of*
2 *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 ven-*
8 *dors, incident response providers, cybersecurity*
9 *insurance entities, and other entities that may*
10 *support covered entities or ransomware attack*
11 *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 Partnership*
18 *Advisory Council established under section 871;*

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

21 *“(C) trade associations;*

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

24 *“(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 rule
5 pursuant to subsection (b)(2), the Director shall re-
6 view the data collected by the Office, and in consulta-
7 tion with other appropriate entities, assess the effec-
8 tiveness 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 re-
12 quired 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 Security
17 and Governmental Affairs of the Senate and the Com-
18 mittee on Homeland Security of the House of Rep-
19 resentatives the results of the evaluation described in
20 paragraph (1) and may thereafter, in accordance
21 with the requirements under subsection (b), publish in
22 the Federal Register a final rule implementing this
23 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 may*
 2 *reorganize and reformat the means by which covered cyber*
 3 *incident reports, ransom payment reports, and any other*
 4 *voluntarily offered information is submitted to the Office.*

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

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

11 *“(b) VOLUNTARY PROVISION OF ADDITIONAL INFOR-*
 12 *MATION IN REQUIRED REPORTS.—Entities may volun-*
 13 *tarily include in reports required under paragraph (1), (2),*
 14 *or (3) of section 2232(a) information that is not required*
 15 *to be included, but may enhance the situational awareness*
 16 *of cyber threats.*

17 *“(c) APPLICATION OF PROTECTIONS.—The protections*
 18 *under section 2235 applicable to covered cyber incident re-*
 19 *ports shall apply in the same manner and to the same ex-*
 20 *tent to reports and information submitted under subsections*
 21 *(a) and (b).*

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

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

1 *obtain information about the incident or ransom payment*
2 *by engaging the entity directly to request information about*
3 *the incident or ransom payment, and if the Director is un-*
4 *able to obtain information through such engagement, by*
5 *issuing a subpoena to the entity, pursuant to subsection (c),*
6 *to gather information sufficient to determine whether a cov-*
7 *ered cyber incident or ransom payment has occurred, and,*
8 *if so, whether additional action is warranted pursuant to*
9 *subsection (d).*

10 “(b) *INITIAL REQUEST FOR INFORMATION.*—

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

23 “(2) *TREATMENT.*—*Information provided to the*
24 *Office in response to a request under paragraph (1)*

1 *shall be treated as if it was submitted through the re-*
2 *porting procedures established in section 2232.*

3 “(c) *AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.*—

4 “(1) *IN GENERAL.*—*If, after the date that is 72*
5 *hours from the date on which the Director made the*
6 *request for information in subsection (b), the Director*
7 *has received no response from the entity from which*
8 *such information was requested, or received an inad-*
9 *equately response, the Director may issue to such entity*
10 *a subpoena to compel disclosure of information the*
11 *Director deems necessary to determine whether a cov-*
12 *ered cyber incident or ransom payment has occurred*
13 *and obtain the information required to be reported*
14 *pursuant to section 2232 and any implementing regu-*
15 *lations.*

16 “(2) *CIVIL ACTION.*—

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

22 “(B) *VENUE.*—*An action under this para-*
23 *graph may be brought in the judicial district in*
24 *which the entity against which the action is*
25 *brought resides, is found, or does business.*

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

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

8 “(4) DEBARMENT OF FEDERAL CONTRACTORS.—
9 If a covered entity with a Federal Government con-
10 tract, grant, or cooperative agreement fails to comply
11 with a subpoena issued under this subsection—

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

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

18 “(d) PROVISION OF CERTAIN INFORMATION TO ATTOR-
19 NEY GENERAL.—

20 “(1) IN GENERAL.—Notwithstanding section
21 2235(a) and subsection (b)(2) of this section, if the
22 Director determines, based on the information pro-
23 vided in response to the subpoena issued pursuant to
24 subsection (c), that the facts relating to the covered
25 cyber incident or ransom payment at issue may con-

1 *stitute grounds for a regulatory enforcement action or*
2 *criminal prosecution, the Director may provide that*
3 *information to the Attorney General or the appro-*
4 *priate regulator, who may use that information for a*
5 *regulatory enforcement action or criminal prosecu-*
6 *tion.*

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

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

21 *“(e) CONSIDERATIONS.—When determining whether to*
22 *exercise the authorities provided under this section, the Di-*
23 *rector shall take into consideration—*

24 *“(1) the size and complexity of the entity;*

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

3 “(3) *prior interaction with the Agency or aware-*
4 *ness of the entity of the policies and procedures of the*
5 *Agency for reporting covered cyber incidents and ran-*
6 *som payments; and*

7 “(4) *for non-covered entities required to submit*
8 *a ransom payment report, the ability of the entity to*
9 *perform a due diligence review pursuant to section*
10 *2232(e).*

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

13 “(g) *REPORT TO CONGRESS.—The Director shall sub-*
14 *mit to Congress an annual report on the number of times*
15 *the Director—*

16 “(1) *issued an initial request for information*
17 *pursuant to subsection (b);*

18 “(2) *issued a subpoena pursuant to subsection*
19 *(c);*

20 “(3) *brought a civil action pursuant to sub-*
21 *section (c)(2); or*

22 “(4) *conducted additional actions pursuant to*
23 *subsection (d).*

1 **“SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO**
2 **THE FEDERAL GOVERNMENT.**

3 *“(a) DISCLOSURE, RETENTION, AND USE.—*

4 *“(1) AUTHORIZED ACTIVITIES.—Information*
5 *provided to the Office or Agency pursuant to section*
6 *2232 may be disclosed to, retained by, and used by,*
7 *consistent with otherwise applicable provisions of*
8 *Federal law, any Federal agency or department, com-*
9 *ponent, officer, employee, or agent of the Federal Gov-*
10 *ernment solely for—*

11 *“(A) a cybersecurity purpose;*

12 *“(B) the purpose of identifying—*

13 *“(i) a cyber threat, including the*
14 *source of the cyber threat; or*

15 *“(ii) a security vulnerability;*

16 *“(C) the purpose of responding to, or other-*
17 *wise preventing or mitigating, a specific threat*
18 *of death, a specific threat of serious bodily harm,*
19 *or a specific threat of serious economic harm, in-*
20 *cluding a terrorist act or a use of a weapon of*
21 *mass destruction;*

22 *“(D) the purpose of responding to, inves-*
23 *tigating, prosecuting, or otherwise preventing or*
24 *mitigating, a serious threat to a minor, includ-*
25 *ing sexual exploitation and threats to physical*
26 *safety; or*

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

7 “(2) AGENCY ACTIONS AFTER RECEIPT.—

8 “(A) RAPID, CONFIDENTIAL SHARING OF
9 CYBER THREAT INDICATORS.—Upon receiving a
10 covered cyber incident or ransom payment report
11 submitted pursuant to this section, the Office
12 shall immediately review the report to determine
13 whether the incident that is the subject of the re-
14 port is connected to an ongoing cyber threat or
15 security vulnerability and where applicable, use
16 such report to identify, develop, and rapidly dis-
17 seminate to appropriate stakeholders actionable,
18 anonymized cyber threat indicators and defen-
19 sive measures.

20 “(B) STANDARDS FOR SHARING SECURITY
21 VULNERABILITIES.—With respect to information
22 in a covered cyber incident or ransom payment
23 report regarding a security vulnerability referred
24 to in paragraph (1)(B)(ii), the Director shall de-
25 velop principles that govern the timing and

1 *manner in which information relating to secu-*
2 *rity vulnerabilities may be shared, consistent*
3 *with common industry best practices and United*
4 *States and international standards.*

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

16 “(A) *personal information of a specific in-*
17 *dividual; or*

18 “(B) *information that identifies a specific*
19 *individual that is not directly related to a cyber-*
20 *security threat.*

21 “(4) *DIGITAL SECURITY.*—*The Office shall ensure*
22 *that reports submitted to the Office pursuant to sec-*
23 *tion 2232, and any information contained in those*
24 *reports, are collected, stored, and protected at a min-*
25 *imum in accordance with the requirements for mod-*

1 *erate impact Federal information systems, as de-*
2 *scribed in Federal Information Processing Standards*
3 *Publication 199, or any successor document.*

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

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

17 “(c) *EXEMPTION FROM DISCLOSURE.—Information*
18 *contained in a report submitted to the Office under section*
19 *2232 shall be exempt from disclosure under section*
20 *552(b)(3)(B) of title 5, United States Code (commonly*
21 *known as the ‘Freedom of Information Act’) and any State,*
22 *Tribal, or local provision of law requiring disclosure of in-*
23 *formation or records.*

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

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

4 “(e) *LIABILITY PROTECTIONS.*—

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

14 “(2) *SCOPE.*—*The liability protections provided*
15 *in subsection (e) shall only apply to or affect litiga-*
16 *tion that is solely based on the submission of a cov-*
17 *ered cyber incident report or ransom payment report*
18 *to the Office.*

19 “(3) *RESTRICTIONS.*—*Notwithstanding para-*
20 *graph (2), no report submitted to the Agency pursu-*
21 *ant to this subtitle or any communication, document,*
22 *material, or other record, created for the sole purpose*
23 *of preparing, drafting, or submitting such report,*
24 *may be received in evidence, subject to discovery, or*
25 *otherwise used in any trial, hearing, or other pro-*

1 *ceeding in or before any court, regulatory body, or*
 2 *other authority of the United States, a State, or a po-*
 3 *litical subdivision thereof, provided that nothing in*
 4 *this subtitle shall create a defense to discovery or oth-*
 5 *erwise affect the discovery of any communication,*
 6 *document, material, or other record not created for*
 7 *the sole purpose of preparing, drafting, or submitting*
 8 *such report.*

9 “(f) *SHARING WITH NON-FEDERAL ENTITIES.—The*
 10 *Agency shall anonymize the victim who reported the infor-*
 11 *mation when making information provided in reports re-*
 12 *ceived under section 2232 available to critical infrastruc-*
 13 *ture owners and operators and the general public.*

14 “(g) *PROPRIETARY INFORMATION.—Information con-*
 15 *tained in a report submitted to the Agency under section*
 16 *2232 shall be considered the commercial, financial, and pro-*
 17 *prietary information of the covered entity when so des-*
 18 *ignated by the covered entity.”.*

19 (c) *TECHNICAL AND CONFORMING AMENDMENT.—The*
 20 *table of contents in section 1(b) of the Homeland Security*
 21 *Act of 2002 (Public Law 107–296; 116 Stat. 2135) is*
 22 *amended by inserting after the items relating to subtitle B*
 23 *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.”.

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

2 (a) *CYBER INCIDENT REPORTING SHARING.*—*Notwith-*
 3 *standing any other provision of law or regulation, any Fed-*
 4 *eral agency that receives a report from an entity of a cyber*
 5 *attack or cyber incident, including a ransomware attack,*
 6 *shall provide all such information to the Director of the Cy-*
 7 *bersecurity Infrastructure Security Agency not later than*
 8 *24 hours after receiving the report, unless a shorter period*
 9 *is required by an agreement made between the Cyber Inci-*
 10 *dent Review Office established under section 2231 of the*
 11 *Homeland Security Act of 2002, as added by section 3(b)*
 12 *of this Act, and another Federal entity.*

13 (b) *CREATION OF COUNCIL.*—*Section 1752(c) of the*
 14 *William M. (Mac) Thornberry National Defense Authoriza-*
 15 *tion Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is amend-*
 16 *ed—*

17 (1) *in paragraph (1)—*

18 (A) *in subparagraph (G), by striking “and”*
 19 *at the end;*

20 (B) *by redesignating subparagraph (H) as*
 21 *subparagraph (I); and*

22 (C) *by inserting after subparagraph (G) the*
 23 *following:*

1 “(H) lead an intergovernmental Cyber Inci-
2 dent Reporting Council, in coordination with the
3 Director of the Office of Management and Budget
4 and the Director of the Cybersecurity and Infra-
5 structure Security Agency and in consultation
6 with Sector Risk Management Agencies (as de-
7 fined in section 2201 of the Homeland Security
8 Act of 2002 (6 U.S.C. 651)) and other appro-
9 priate Federal agencies, to coordinate, deconflict,
10 and harmonize Federal incident reporting re-
11 quirements, including those issued through regu-
12 lations, for covered entities (as defined in section
13 2230 of such Act) and entities that make a ran-
14 som payment (as defined in such section 2201 (6
15 U.S.C. 651)); and”;

16 (2) by adding at the end the following:

17 “(3) *RULE OF CONSTRUCTION.*—Nothing in
18 paragraph (1)(H) shall be construed to provide any
19 additional regulatory authority to any Federal enti-
20 ty.”.

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

1 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of
2 Management and Budget, to the maximum extent prac-
3 ticable—

4 (1) periodically review existing regulatory re-
5 quirements, including the information required in
6 such reports, to report cyber incidents and ensure that
7 any such reporting requirements and procedures
8 avoid conflicting, duplicative, or burdensome require-
9 ments; and

10 (2) coordinate with the Director and regulatory
11 authorities that receive reports relating to cyber inci-
12 dents to identify opportunities to streamline reporting
13 processes, and where feasible, facilitate interagency
14 agreements between such authorities to permit the
15 sharing of such reports, consistent with applicable
16 law and policy, without impacting the ability of such
17 agencies to gain timely situational awareness of a
18 covered cyber incident or ransom payment.

19 **SEC. 5. RANSOMWARE VULNERABILITY WARNING PILOT**
20 **PROGRAM.**

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

1 *tifying information systems that contain security*
2 *vulnerabilities associated with common ransomware at-*
3 *tacks, and to notify the owners of those vulnerable systems*
4 *of their security vulnerability.*

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

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

10 (2) *utilize existing authorities to identify Fed-*
11 *eral and other relevant information systems that con-*
12 *tain the security vulnerabilities identified in para-*
13 *graph (1).*

14 (c) *ENTITY NOTIFICATION.—*

15 (1) *IDENTIFICATION.—If the Director is able to*
16 *identify the entity at risk that owns or operates a*
17 *vulnerable information system identified in subsection*
18 *(b), the Director may notify the owner of the informa-*
19 *tion system.*

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

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

3 (3) *REQUIRED INFORMATION.*—*A notification*
4 *made under paragraph (1) shall include information*
5 *on the identified security vulnerability and mitiga-*
6 *tion techniques.*

7 (d) *PRIORITIZATION OF NOTIFICATIONS.*—*To the ex-*
8 *tent practical, the Director shall prioritize covered entities*
9 *for identification and notification activities under the pilot*
10 *program established under this section.*

11 (e) *LIMITATION ON PROCEDURES.*—*No procedure, no-*
12 *tification, or other authorities utilized in the execution of*
13 *the pilot program established under subsection (a) shall re-*
14 *quire an owner or operator of a vulnerable information sys-*
15 *tem to take any action as a result of a notice of a security*
16 *vulnerability made pursuant to subsection (c).*

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

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

21 (a) *JOINT RANSOMWARE TASK FORCE.*—

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

1 *nationwide campaign against ransomware attacks,*
2 *and identify and pursue opportunities for inter-*
3 *national cooperation.*

4 (2) *COMPOSITION.*—*The Joint Ransomware Task*
5 *Force shall consist of participants from Federal agen-*
6 *cies, as determined appropriate by the National*
7 *Cyber Director in consultation with the Secretary of*
8 *Homeland Security.*

9 (3) *RESPONSIBILITIES.*—*The Joint Ransomware*
10 *Task Force, utilizing only existing authorities of each*
11 *participating agency, shall coordinate across the Fed-*
12 *eral Government the following activities:*

13 (A) *Prioritization of intelligence-driven op-*
14 *erations to disrupt specific ransomware actors.*

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

20 (C) *Identifying, in consultation with rel-*
21 *evant entities, a list of highest threat*
22 *ransomware entities updated on an ongoing*
23 *basis, in order to facilitate—*

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

1 (ii) identify metrics for success of said
2 actions.

3 (D) Disrupting ransomware criminal ac-
4 tors, associated infrastructure, and their fi-
5 nances.

6 (E) Facilitating coordination and collabo-
7 ration between Federal entities and relevant en-
8 tities, including the private sector, to improve
9 Federal actions against ransomware threats.

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

12 (G) Creation of after-action reports and
13 other lessons learned from Federal actions that
14 identify successes and failures to improve subse-
15 quent actions.

16 (H) Any other activities determined appro-
17 priate by the task force to mitigate the threat of
18 ransomware attacks against Federal and non-
19 Federal entities.

20 (b) *CLARIFYING PRIVATE-SECTOR LAWFUL DEFENSIVE*
21 *MEASURES.*—Not later than 180 days after the date of en-
22 actment of this Act, the National Cyber Director, in coordi-
23 nation with the Secretary of Homeland Security and the
24 Attorney General, shall submit to the Committee on Home-
25 land Security and Governmental Affairs and the Committee

1 *on the Judiciary of the Senate and the Committee on Home-*
2 *land Security, the Committee on the Judiciary, and the*
3 *Committee on Oversight and Reform of the House of Rep-*
4 *resentatives a report that describes defensive measures that*
5 *private-sector actors can take when countering ransomware*
6 *attacks and what laws need to be clarified to enable that*
7 *action.*

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

11 **SEC. 7. CONGRESSIONAL REPORTING.**

12 (a) *REPORT ON STAKEHOLDER ENGAGEMENT.*—*Not*
13 *later than 30 days after the date on which the Director*
14 *issues the interim final rule under section 2232(b)(1) of the*
15 *Homeland Security Act of 2002, as added by section 3(b)*
16 *of this Act, the Director shall submit to the Committee on*
17 *Homeland Security and Government Affairs of the Senate*
18 *and the Committee on Homeland Security of the House of*
19 *Representatives a report that describes how the Director en-*
20 *gaged stakeholders in the development of the interim final*
21 *rule.*

22 (b) *REPORT ON OPPORTUNITIES TO STRENGTHEN SE-*
23 *curity RESEARCH.*—*Not later than 1 year after the date*
24 *of enactment of this Act, the Director shall submit to the*
25 *Committee on Homeland Security and Government Affairs*

1 *of the Senate and the Committee on Homeland Security of*
2 *the House of Representatives a report describing how the*
3 *Cyber Incident Review Office has carried out activities*
4 *under section 2231(b)(9) of the Homeland Security Act of*
5 *2002, as added by section 3(b) of this Act, by proactively*
6 *identifying opportunities to use cyber incident data to in-*
7 *form and enabling cybersecurity research within the aca-*
8 *demic and private sector.*

9 (c) *REPORT ON RANSOMWARE VULNERABILITY WARN-*
10 *ING PILOT PROGRAM.*—*Not later than 1 year after the date*
11 *of enactment of this Act, and annually thereafter for the*
12 *duration of the pilot program established under section 5,*
13 *the Director shall submit to the Committee on Homeland*
14 *Security and Governmental Affairs of the Senate and the*
15 *Committee on Homeland Security of the House of Rep-*
16 *resentatives a report, which may include a classified annex,*
17 *on the effectiveness of the pilot program, which shall include*
18 *a discussion of the following:*

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

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

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

1 (4) *To the extent practicable, the number of vul-*
2 *nerable devices or systems mitigated under this pilot*
3 *by the Agency during the preceding year.*

4 (d) *REPORT ON HARMONIZATION OF REPORTING REG-*
5 *ULATIONS.—*

6 (1) *IN GENERAL.—Not later than 180 days after*
7 *the date on which the National Cyber Director con-*
8 *venes the Council described in section 1752(c)(1)(H)*
9 *of the William M. (Mac) Thornberry National Defense*
10 *Authorization Act for Fiscal Year 2021 (6 U.S.C.*
11 *1500(c)(1)(H)), the National Cyber Director shall*
12 *submit to the appropriate congressional committees a*
13 *report that includes—*

14 (A) *a list of duplicative Federal cyber inci-*
15 *dent reporting requirements on covered entities*
16 *and entities that make a ransom payment;*

17 (B) *a description of any challenges in har-*
18 *monizing the duplicative reporting requirements;*

19 (C) *any actions the National Cyber Director*
20 *intends to take to facilitate harmonizing the du-*
21 *plicative reporting requirements; and*

22 (D) *any proposed legislative changes nec-*
23 *essary to address the duplicative reporting.*

1 (2) *RULE OF CONSTRUCTION.*—*Nothing in para-*
2 *graph (1) shall be construed to provide any addi-*
3 *tional regulatory authority to any Federal agency.*

4 (e) *GAO REPORT.*—*Not later than 2 years after the*
5 *date of enactment of this Act, the Comptroller General of*
6 *the United States shall submit to the Committee on Home-*
7 *land Security and Governmental Affairs of the Senate and*
8 *the Committee on Homeland Security of the House of Rep-*
9 *resentatives a report on the implementation of this Act and*
10 *the amendments made by this Act.*

Calendar No. 633

117TH CONGRESS
2^D SESSION

S. 2875

[Report No. 117-249]

A BILL

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

DECEMBER 13, 2022

Reported with an amendment