

.....
(Original Signature of Member)

117TH CONGRESS
1ST SESSION

H. R.

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 HOUSE OF REPRESENTATIVES

Ms. CLARKE of New York (for herself and Mr. KATKO) introduced the following bill; which was referred to the Committee on

A BILL

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

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

3 **SECTION 1. SHORT TITLE.**

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

1 **SEC. 2. CYBER INCIDENT REVIEW OFFICE.**

2 (a) IN GENERAL.—Subtitle A of title XXII of the
3 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
4 is amended by adding at the end the following new section:

5 **“SEC. 2220A. CYBER INCIDENT REVIEW OFFICE.**

6 “(a) DEFINITIONS.—In this section:

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

14 “(2) COVERED ENTITY.—The term ‘covered en-
15 tity’ means an entity that owns or operates critical
16 infrastructure that satisfies the definition estab-
17 lished by the Director in the reporting requirements
18 and procedures issued pursuant to subsection (d).

19 “(3) COVERED CYBSECURITY INCIDENT.—The
20 term ‘covered cybersecurity incident’ means a cyber-
21 security incident experienced by a covered entity
22 that satisfies the definition and criteria established
23 by the Director in the reporting requirements and
24 procedures issued pursuant to subsection (d).

25 “(4) CYBER THREAT INDICATOR.—The term
26 ‘cyber threat indicator’ has the meaning given such

1 term in section 102 of the Cybersecurity Act of 2015
2 (enacted as division N of the Consolidated Appro-
3 priations Act, 2016 (Public Law 114–113; 6 U.S.C.
4 1501)).

5 “(5) CYBERSECURITY PURPOSE.—The term ‘cy-
6 bersecurity purpose’ has the meaning given such
7 term in section 102 of the Cybersecurity Act of 2015
8 (enacted as division N of the Consolidated Appro-
9 priations Act, 2016 (Public Law 114-113; 6 U.S.C.
10 1501)).

11 “(6) CYBERSECURITY THREAT.—The term ‘cy-
12 bersecurity threat’ has the meaning given such term
13 in section 102 of the Cybersecurity Act of 2015 (en-
14 acted as division N of the Consolidated Appropria-
15 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
16 1501)).

17 “(7) DEFENSIVE MEASURE.—The term ‘defen-
18 sive measure’ has the meaning given such term in
19 section 102 of the Cybersecurity Act of 2015 (en-
20 acted as division N of the Consolidated Appropria-
21 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
22 1501)).

23 “(8) INFORMATION SHARING AND ANALYSIS OR-
24 GANIZATION.—The term ‘Information Sharing and

1 Analysis Organization’ has the meaning given such
2 term in section 2222(5).

3 “(9) INFORMATION SYSTEM.—The term ‘infor-
4 mation system’ has the meaning given such term in
5 section 102 of the Cybersecurity Act of 2015 (en-
6 acted as division N of the Consolidated Appropria-
7 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
8 1501(9)).

9 “(10) INTELLIGENCE COMMUNITY.—The term
10 ‘intelligence community’ has the meaning given the
11 term in section 3(4) of the National Security Act of
12 1947 (50 U.S.C. 3003(4)).

13 “(11) MANAGED SERVICE PROVIDER.—The
14 term ‘managed service provider’ means an entity
15 that delivers services, such as network, application,
16 infrastructure, or security services, via ongoing and
17 regular support and active administration on cus-
18 tomers’ premises, in the managed service provider’s
19 data center (such as hosting), or in a third-party
20 data center.

21 “(12) SECURITY CONTROL.—The term ‘security
22 control’ has the meaning given such term in section
23 102 of the Cybersecurity Act of 2015 (enacted as di-
24 vision N of the Consolidated Appropriations Act,
25 2016 (Public Law 114–113; 6 U.S.C. 1501)).

1 “(13) SECURITY VULNERABILITY.—The term
2 ‘security vulnerability’ has the meaning given such
3 term in section 102 of the Cybersecurity Act of 2015
4 (enacted as division N of the Consolidated Appro-
5 priations Act, 2016 (Public Law 114–113; 6 U.S.C.
6 1501)).

7 “(14) SIGNIFICANT CYBER INCIDENT.—The
8 term ‘significant cyber incident’ means a cyber inci-
9 dent, or a group of related cyber incidents, that the
10 Director determines is likely to result in demon-
11 strable harm to the national security interests, for-
12 eign relations, or economy of the United States or
13 to the public confidence, civil liberties, or public
14 health and safety of the American people.

15 “(15) SUPPLY CHAIN ATTACK.—The term ‘sup-
16 ply chain attack’ means an attack that allows an ad-
17 versary to utilize implants or other vulnerabilities in-
18 serted prior to installation in order to infiltrate data,
19 or manipulate information technology hardware,
20 software, operating systems, peripherals (such as in-
21 formation technology products), or services at any
22 point during the life cycle.

23 “(b) CYBER INCIDENT REVIEW OFFICE.—There is
24 established in the Agency a Cyber Incident Review Office
25 (in this section referred to as the ‘Office’) to receive, ag-

1 gregate, and analyze reports related to covered cybersecu-
2 rity incidents submitted by covered entities in furtherance
3 of the activities specified in subsection (c) of this section
4 and sections 2202(e), 2209(c), and 2203 to enhance the
5 situational awareness of cybersecurity threats across crit-
6 ical infrastructure sectors.

7 “(c) ACTIVITIES.—The Office shall, in furtherance of
8 the activities specified in sections 2202(e), 2209(c), and
9 2203—

10 “(1) receive, aggregate, analyze, and secure re-
11 ports from covered entities related to a covered cy-
12 bersecurity incident to assess the effectiveness of se-
13 curity controls and identify tactics, techniques, and
14 procedures adversaries use to overcome such con-
15 trols;

16 “(2) facilitate the timely sharing between rel-
17 evant critical infrastructure owners and operators
18 and, as appropriate, the intelligence community of
19 information relating to covered cybersecurity inci-
20 dents, particularly with respect to an ongoing cyber-
21 security threat or security vulnerability;

22 “(3) for a covered cybersecurity incident that
23 also satisfies the definition of a significant cyber in-
24 cident, or are part of a group of related cyber inci-
25 dents that together satisfy such definition, conduct

1 a review of the details surrounding such covered cy-
2 bersecurity incident or group of such incidents and
3 identify ways to prevent or mitigate similar incidents
4 in the future;

5 “(4) with respect to covered cybersecurity inci-
6 dent reports under subsection (d) involving an ongo-
7 ing cybersecurity threat or security vulnerability, im-
8 mediately review such reports for cyber threat indi-
9 cators that can be anonymized and disseminated,
10 with defensive measures, to appropriate stake-
11 holders, in coordination with other Divisions within
12 the Agency, as appropriate;

13 “(5) publish quarterly unclassified, public re-
14 ports that describe aggregated, anonymized observa-
15 tions, findings, and recommendations based on cov-
16 ered cybersecurity incident reports under subsection
17 (d); and

18 “(6) proactively identify opportunities, in ac-
19 cordance with the protections specified in sub-
20 sections (e) and (f), to leverage and utilize data on
21 cybersecurity incidents in a manner that enables and
22 strengthens cybersecurity research carried out by
23 academic institutions and other private sector orga-
24 nizations, to the greatest extent practicable.

1 “(d) COVERED CYBERSECURITY INCIDENT REPORT-
2 ING REQUIREMENTS AND PROCEDURES.—

3 “(1) IN GENERAL.—Not later than 270 days
4 after the date of the enactment of this section, the
5 Director, in consultation with Sector Risk Manage-
6 ment Agencies and the heads of other Federal de-
7 partments and agencies, as appropriate, shall, after
8 a 60 day consultative period, followed by a 90 day
9 comment period with appropriate stakeholders, pub-
10 lish in the Federal Register an interim final rule im-
11 plementing this section. Notwithstanding section 553
12 of title 5, United States Code, such rule shall be ef-
13 fective, on an interim basis, immediately upon publi-
14 cation, but may be subject to change and revision
15 after public notice and opportunity for comment.
16 The Director shall issue a final rule not later than
17 one year after publication of such interim final rule.
18 Such interim final rule shall—

19 “(A) require covered entities to submit to
20 the Office reports containing information relat-
21 ing to covered cybersecurity incidents; and

22 “(B) establish procedures that clearly de-
23 scribe—

24 “(i) the types of critical infrastructure
25 entities determined to be covered entities;

1 “(ii) the types of cybersecurity inci-
2 dents determined to be covered cybersecu-
3 rity incidents;

4 “(iii) the mechanisms by which cov-
5 ered cybersecurity incident reports under
6 subparagraph (A) are to be submitted, in-
7 cluding—

8 “(I) the contents, described in
9 paragraph (4), to be included in each
10 such report, including any supple-
11 mental reporting requirements;

12 “(II) the timing relating to when
13 each such report should be submitted;
14 and

15 “(III) the format of each such re-
16 port;

17 “(iv) describe the manner in which
18 the Office will carry out enforcement ac-
19 tions under subsection (g), including with
20 respect to the issuance of subpoenas, con-
21 ducting examinations, and other aspects
22 relating to noncompliance; and

23 “(v) any other responsibilities to be
24 carried out by covered entities, or other

1 procedures necessary to implement this
2 section.

3 “(2) COVERED ENTITIES.—In determining
4 which types of critical infrastructure entities are cov-
5 ered entities for purposes of this section, the Sec-
6 retary, acting through the Director, in consultation
7 with Sector Risk Management Agencies and the
8 heads of other Federal departments and agencies, as
9 appropriate, shall consider—

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

14 “(B) the likelihood that such an entity
15 may be targeted by a malicious cyber actor, in-
16 cluding a foreign country;

17 “(C) the extent to which damage, disrup-
18 tion, or unauthorized access to such and entity
19 will disrupt the reliable operation of other crit-
20 ical infrastructure assets; and

21 “(D) the extent to which an entity or sec-
22 tor is subject to existing regulatory require-
23 ments to report cybersecurity incidents, and the
24 possibility of coordination and sharing of re-
25 ports between the Office and the regulatory au-

1 thority to which such entity submits such other
2 reports.

3 “(3) OUTREACH TO COVERED ENTITIES.—

4 “(A) IN GENERAL.—The Director shall
5 conduct an outreach and education campaign to
6 inform covered entities of the requirements of
7 this section.

8 “(B) ELEMENTS.—The outreach and edu-
9 cation campaign under subparagraph (A) shall
10 include the following:

11 “(i) Overview of the interim final rule
12 and final rule issued pursuant to this sec-
13 tion.

14 “(ii) Overview of reporting require-
15 ments and procedures issued pursuant to
16 paragraph (1).

17 “(iii) Overview of mechanisms to sub-
18 mit to the Office covered cybersecurity inci-
19 dent reports and information relating to
20 the disclosure, retention, and use of inci-
21 dent reports under this section.

22 “(iv) Overview of the protections af-
23 forded to covered entities for complying
24 with requirements under subsection (f).

1 “(v) Overview of the steps taken
2 under subsection (g) when a covered entity
3 is not in compliance with the reporting re-
4 quirements under paragraph (1).

5 “(C) COORDINATION.—The Director may
6 conduct the outreach and education campaign
7 under subparagraph (A) through coordination
8 with the following:

9 “(i) The Critical Infrastructure Part-
10 nership Advisory Council established pur-
11 suant to section 871.

12 “(ii) Information Sharing and Anal-
13 ysis Organizations.

14 “(iii) Any other means the Director
15 determines to be effective to conduct such
16 campaign.

17 “(4) COVERED CYBERSECURITY INCIDENTS.—

18 “(A) CONSIDERATIONS.—In accordance
19 with subparagraph (B), in determining which
20 types of incidents are covered cybersecurity inci-
21 dents for purposes of this section, the Direc-
22 tor shall consider—

23 “(i) the sophistication or novelty of
24 the tactics used to perpetrate such an inci-

1 dent, as well as the type, volume, and sen-
2 sitivity of the data at issue;

3 “(ii) the number of individuals di-
4 rectly or indirectly affected or potentially
5 affected by such an incident; and

6 “(iii) potential impacts on industrial
7 control systems, such as supervisory con-
8 trol and data acquisition systems, distrib-
9 uted control systems, and programmable
10 logic controllers.

11 “(B) MINIMUM THRESHOLDS.—For a cy-
12 bersecurity incident to be considered a covered
13 cybersecurity incident a cybersecurity incident
14 shall, at a minimum, include at least one of the
15 following:

16 “(i) Unauthorized access to an infor-
17 mation system or network that leads to
18 loss of confidentiality, integrity, or avail-
19 ability of such information system or net-
20 work, or has a serious impact on the safety
21 and resiliency of operational systems and
22 processes.

23 “(ii) Disruption of business or indus-
24 trial operations due to a distributed denial
25 of service attack, a ransomware attack, or

1 exploitation of a zero-day vulnerability,
2 against—

3 “(I) an information system or
4 network; or

5 “(II) an operational technology
6 system or process.

7 “(iii) Unauthorized access or disrup-
8 tion of business or industrial operations
9 due to loss of service facilitated through,
10 or caused by a compromise of, a cloud
11 service provider, managed service provider,
12 other third-party data hosting provider, or
13 supply chain attack.

14 “(5) REPORTS.—

15 “(A) TIMING.—

16 “(i) IN GENERAL.—The Director, in
17 consultation with Sector Risk Management
18 Agencies and the heads of other Federal
19 departments and agencies, as appropriate,
20 shall establish reporting timelines for cov-
21 ered entities to submit promptly to the Of-
22 fice covered cybersecurity incident reports,
23 as the Director determines reasonable and
24 appropriate based on relevant factors, such
25 as the nature of the covered cybersecurity

1 incident at issue and the time required for
2 investigation, but in no case may the Di-
3 rector require reporting by a covered entity
4 earlier than 72 hours after confirmation
5 that a covered cybersecurity incident has
6 occurred.

7 “(ii) CONSIDERATIONS.—In deter-
8 mining reporting timelines under clause
9 (i), the Director shall—

10 “(I) consider any existing regu-
11 latory reporting requirements, similar
12 in scope purpose, and timing to the
13 reporting requirements under this sec-
14 tion, to which a covered entity may
15 also be subject, and make efforts to
16 harmonize the timing and contents of
17 any such reports to the maximum ex-
18 tent practicable; and

19 “(II) balance the Agency’s need
20 for situational awareness with a cov-
21 ered entity’s ability to conduct inci-
22 dent response and investigations.

23 “(B) THIRD PARTY REPORTING.—

24 “(i) IN GENERAL.—Covered entities
25 may submit a covered cybersecurity inci-

1 dent report through a third party entity or
2 Information Sharing and Analysis Organi-
3 zation.

4 “(ii) DUTY TO ENSURE COMPLI-
5 ANCE.—Third party reporting under this
6 subparagraph does not relieve a covered
7 entity of the duty to ensure compliance
8 with the requirements of this paragraph.

9 “(C) SUPPLEMENTAL REPORTING.—Cov-
10 ered entities shall submit promptly to the Office
11 an update or supplement to a previously sub-
12 mitted covered cybersecurity incident report if
13 new or different information becomes available
14 that would otherwise have been required to have
15 been included in such previously submitted re-
16 port. In determining reporting timelines, the
17 Director may choose to establish a flexible,
18 phased reporting timeline for covered entities to
19 report information in a manner that aligns with
20 investigative timelines and allows covered enti-
21 ties to prioritize incident response efforts over
22 compliance.

23 “(D) CONTENTS.—Covered cybersecurity
24 incident reports submitted pursuant to this sec-
25 tion shall contain such information as the Di-

1 rector prescribes, including the following infor-
2 mation, to the extent applicable and available,
3 with respect to a covered cybersecurity incident:

4 “(i) A description of the covered cy-
5 bersecurity incident, including identifica-
6 tion of the affected information systems,
7 networks, or devices that were, or are rea-
8 sonably believed to have been, affected by
9 such incident, and the estimated date
10 range of such incident.

11 “(ii) Where applicable, a description
12 of the vulnerabilities, tactics, techniques,
13 and procedures relevant to such incident.

14 “(iii) Where applicable, any identi-
15 fying information related to the actor re-
16 sponsible for such incident.

17 “(iv) Where applicable, identification
18 of the category or categories of information
19 that was, or is reasonably believed to have
20 been, accessed or acquired by an unauthor-
21 ized person.

22 “(v) Contact information, such as
23 telephone number or electronic mail ad-
24 dress, that the Office may use to contact
25 the covered entity or agent of such covered

1 entity, or, where applicable, the service
2 provider of such covered entity.

3 “(6) RESPONSIBILITIES OF COVERED ENTI-
4 TIES.—Covered entities that experience a covered cy-
5 bersecurity incident shall coordinate with the Office
6 to the extent necessary to comply with this section,
7 and, to the extent practicable, cooperate with the Of-
8 fice in a manner that supports enhancing the Agen-
9 cy’s situational awareness of cybersecurity threats
10 across critical infrastructure sectors.

11 “(7) HARMONIZING REPORTING REQUIRE-
12 MENTS.—In establishing the reporting requirements
13 and procedures under paragraph (1), the Director
14 shall, to the maximum extent practicable—

15 “(A) review existing regulatory require-
16 ments, including the information required in
17 such reports, to report cybersecurity incidents
18 that may apply to covered entities, and ensure
19 that any such reporting requirements and pro-
20 cedures avoid conflicting, duplicative, or bur-
21 densome requirements; and

22 “(B) coordinate with other regulatory au-
23 thorities that receive reports relating to cyberse-
24 curity incidents to identify opportunities to
25 streamline reporting processes, and where fea-

1 sible, enter into agreements with such authori-
2 ties to permit the sharing of such reports with
3 the Office, consistent with applicable law and
4 policy, without impacting the Office’s ability to
5 gain timely situational awareness of a covered
6 cybersecurity incident or significant cyber inci-
7 dent.

8 “(e) DISCLOSURE, RETENTION, AND USE OF INCI-
9 DENT REPORTS.—

10 “(1) AUTHORIZED ACTIVITIES.—No informa-
11 tion provided to the Office in accordance with sub-
12 sections (d) or (h) may be disclosed to, retained by,
13 or used by any Federal department or agency, or
14 any component, officer, employee, or agent of the
15 Federal Government, except if the Director deter-
16 mines such disclosure, retention, or use is necessary
17 for—

18 “(A) a cybersecurity purpose;

19 “(B) the purpose of identifying—

20 “(i) a cybersecurity threat, including
21 the source of such threat; or

22 “(ii) a security vulnerability;

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

1 “(i) death;

2 “(ii) serious bodily harm; or

3 “(iii) serious economic harm, includ-
4 ing a terrorist act or a use of a weapon of
5 mass destruction;

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

11 “(E) the purpose of preventing, inves-
12 tigating, disrupting, or prosecuting an offense
13 related to a threat—

14 “(i) described in subparagraphs (B)
15 through (D); or

16 “(ii) specified in section
17 105(d)(5)(A)(v) of the Cybersecurity Act
18 of 2015 (enacted as division N of the Con-
19 solidated Appropriations Act, 2016 (Public
20 Law 114–113; 6 U.S.C.
21 1504(d)(5)(A)(v))).

22 “(2) EXCEPTIONS.—

23 “(A) RAPID, CONFIDENTIAL SHARING OF
24 CYBER THREAT INDICATORS.—Upon receiving a
25 covered cybersecurity incident report submitted

1 pursuant to this section, the Office shall imme-
2 diately review such report to determine whether
3 the incident that is the subject of such report
4 is connected to an ongoing cybersecurity threat
5 or security vulnerability and where applicable,
6 use such report to identify, develop, and rapidly
7 disseminate to appropriate stakeholders action-
8 able, anonymized cyber threat indicators and
9 defensive measures.

10 “(B) STANDARDS FOR SHARING SECURITY
11 VULNERABILITIES.—With respect to informa-
12 tion in a covered cybersecurity incident report
13 regarding a security vulnerability referred to in
14 paragraph (1)(B)(ii), the Director shall develop
15 principles that govern the timing and manner in
16 which information relating to security
17 vulnerabilities may be shared, consistent with
18 common industry best practices and United
19 States and international standards.

20 “(3) PRIVACY AND CIVIL LIBERTIES.—Informa-
21 tion contained in reports submitted to the Office
22 pursuant to subsections (d) and (h) shall be re-
23 tained, used, and disseminated, where permissible
24 and appropriate, by the Federal Government in a
25 manner consistent with processes for the protection

1 of personal information adopted pursuant to section
2 105 of the Cybersecurity Act of 2015 (enacted as di-
3 vision N of the Consolidated Appropriations Act,
4 2016 (Public Law 114–113; 6 U.S.C. 1504)).

5 “(4) PROHIBITION ON USE OF INFORMATION IN
6 REGULATORY ACTIONS.—

7 “(A) IN GENERAL.—Information contained
8 in reports submitted to the Office pursuant to
9 subsections (d) and (h) may not be used by any
10 Federal, State, Tribal, or local government to
11 regulate, including through an enforcement ac-
12 tion, the lawful activities of any non-Federal en-
13 tity.

14 “(B) EXCEPTION.—A report submitted to
15 the Agency pursuant to subsection (d) or (h)
16 may, consistent with Federal or State regu-
17 latory authority specifically relating to the pre-
18 vention and mitigation of cybersecurity threats
19 to information systems, inform the development
20 or implementation of regulations relating to
21 such systems.

22 “(f) PROTECTIONS FOR REPORTING ENTITIES AND
23 INFORMATION.—Reports describing covered cybersecurity
24 incidents submitted to the Office by covered entities in ac-
25 cordance with subsection (d), as well as voluntarily-sub-

1 mitted cybersecurity incident reports submitted to the Of-
2 fice pursuant to subsection (h), shall be—

3 “(1) entitled to the protections against liability
4 described in section 106 of the Cybersecurity Act of
5 2015 (enacted as division N of the Consolidated Ap-
6 propriations Act, 2016 (Public Law 114–113; 6
7 U.S.C. 1505));

8 “(2) exempt from disclosure under section 552
9 of title 5, United States Code, as well as any provi-
10 sion of State, Tribal, or local freedom of information
11 law, open government law, open meetings law, open
12 records law, sunshine law, or similar law requiring
13 disclosure of information or records; and

14 “(3) considered the commercial, financial, and
15 proprietary information of the covered entity when
16 so designated by the covered entity.

17 “(g) NONCOMPLIANCE WITH REQUIRED REPORT-
18 ING.—

19 “(1) PURPOSE.—In the event a covered entity
20 experiences a cybersecurity incident but does not
21 comply with the reporting requirements under this
22 section, the Director may obtain information about
23 such incident by engaging directly such covered enti-
24 ty in accordance with paragraph (2) to request in-
25 formation about such incident, or, if the Director is

1 unable to obtain such information through such en-
2 gagement, by issuing a subpoena to such covered en-
3 tity, subject to paragraph (3), to gather information
4 sufficient to determine whether such incident is a
5 covered cybersecurity incident, and if so, whether ad-
6 ditional action is warranted pursuant to paragraph
7 (4).

8 “(2) INITIAL REQUEST FOR INFORMATION.—

9 “(A) IN GENERAL.—If the Director has
10 reason to believe, whether through public re-
11 porting, intelligence gathering, or other infor-
12 mation in the Federal Government’s possession,
13 that a covered entity has experienced a cyberse-
14 curity incident that may be a covered cyberse-
15 curity incident but did not submit pursuant to
16 subsection (d) to the Office a covered cyberse-
17 curity incident report relating thereto, the Di-
18 rector may request information from such cov-
19 ered entity to confirm whether the cybersecurity
20 incident at issue is a covered cybersecurity inci-
21 dent, and determine whether further examina-
22 tion into the details surrounding such incident
23 are warranted pursuant to paragraph (4).

24 “(B) TREATMENT.—Information provided
25 to the Office in response to a request under

1 subparagraph (A) shall be treated as if such in-
2 formation was submitted pursuant to the re-
3 porting procedures established in accordance
4 with subsection (d).

5 “(3) AUTHORITY TO ISSUE SUBPOENAS.—

6 “(A) IN GENERAL.—If, after the date that
7 is seven days from the date on which the Direc-
8 tor made a request for information in para-
9 graph (2), the Director has received no re-
10 sponse from the entity from which such infor-
11 mation was requested, or received an inad-
12 equate response, the Director may issue to such
13 entity a subpoena to compel disclosure of infor-
14 mation the Director considers necessary to de-
15 termine whether a covered cybersecurity inci-
16 dent has occurred and assess potential impacts
17 to national security, economic security, or pub-
18 lic health and safety, determine whether further
19 examination into the details surrounding such
20 incident are warranted pursuant to paragraph
21 (4), and if so, compel disclosure of such infor-
22 mation as is necessary to carry out activities
23 described in subsection (c).

24 “(B) CIVIL ACTION.—If a covered entity
25 does not comply with a subpoena, the Director

1 may bring a civil action in a district court of
2 the United States to enforce such subpoena. An
3 action under this paragraph may be brought in
4 the judicial district in which the entity against
5 which the action is brought resides, is found, or
6 does business. The court may punish a failure
7 to obey an order of the court to comply with the
8 subpoena as a contempt of court.

9 “(C) NON-APPLICABILITY OF PROTEC-
10 TIONS.—The protections described in subsection
11 (f) do not apply to a covered entity that is the
12 recipient of a subpoena under this paragraph
13 (3).

14 “(4) ADDITIONAL ACTIONS.—

15 “(A) EXAMINATION.—If, based on the in-
16 formation provided in response to a subpoena
17 issued pursuant to paragraph (3), the Director
18 determines that the cybersecurity incident at
19 issue is a significant cyber incident, or is part
20 of a group of related cybersecurity incidents
21 that together satisfy the definition of a signifi-
22 cant cyber incident, and a more thorough exam-
23 ination of the details surrounding such incident
24 is warranted in order to carry out activities de-
25 scribed in subsection (c), the Director may di-

1 rect the Office to conduct an examination of
2 such incident in order to enhance the Agency’s
3 situational awareness of cybersecurity threats
4 across critical infrastructure sectors, in a man-
5 ner consistent with privacy and civil liberties
6 protections under applicable law.

7 “(B) PROVISION OF CERTAIN INFORMA-
8 TION TO ATTORNEY GENERAL.—Notwith-
9 standing subsection (e)(4) and paragraph
10 (2)(B), if the Director determines, based on the
11 information provided in response to a subpoena
12 issued pursuant to paragraph (3) or identified
13 in the course of an examination under subpara-
14 graph (A), that the facts relating to the cyber-
15 security incident at issue may constitute
16 grounds for a regulatory enforcement action or
17 criminal prosecution, the Director may provide
18 such information to the Attorney General or the
19 appropriate regulator, who may use such infor-
20 mation for a regulatory enforcement action or
21 criminal prosecution.

22 “(h) VOLUNTARY REPORTING OF CYBER INCI-
23 DENTS.—The Agency shall receive cybersecurity incident
24 reports submitted voluntarily by entities that are not cov-
25 ered entities, or concerning cybersecurity incidents that do

1 not satisfy the definition of covered cybersecurity incidents
2 but may nevertheless enhance the Agency’s situational
3 awareness of cybersecurity threats across critical infra-
4 structure sectors. The protections under this section appli-
5 cable to covered cybersecurity incident reports shall apply
6 in the same manner and to the same extent to voluntarily-
7 submitted cybersecurity incident reports under this sub-
8 section.

9 “(i) NOTIFICATION TO IMPACTED COVERED ENTI-
10 TIES.—If the Director receives information regarding a
11 cybersecurity incident impacting a Federal agency relating
12 to unauthorized access to data provided to such Federal
13 agency by a covered entity, and with respect to which such
14 incident is likely to undermine the security of such covered
15 entity or cause operational or reputational damage to such
16 covered entity, the Director shall, to the extent prac-
17 ticable, notify such covered entity and provide to such cov-
18 ered entity such information regarding such incident as
19 is necessary to enable such covered entity to address any
20 such security risk or operational or reputational damage
21 arising from such incident.

22 “(j) EXEMPTION.—Subchapter I of chapter 35 of
23 title 44, United States Code, does not apply to any action
24 to carry out this section.”.

25 (b) REPORTS.—

1 (1) ON STAKEHOLDER ENGAGEMENT.—Not
2 later than 30 days before the date on which that the
3 Director of the Cybersecurity and Infrastructure Se-
4 curity Agency of the Department of Homeland Secu-
5 rity intends to issue an interim final rule under sub-
6 section (d)(1) of section 2220A of the Homeland Se-
7 curity Act of 2002 (as added by subsection (a)), the
8 Director shall submit to the Committee on Home-
9 land Security of the House of Representatives and
10 the Committee on Homeland Security and Govern-
11 mental Affairs of the Senate a report that describes
12 how the Director engaged stakeholders in the devel-
13 opment of such interim final rules.

14 (2) ON OPPORTUNITIES TO STRENGTHEN CY-
15 BERSECURITY RESEARCH.—Not later than one year
16 after the date of the enactment of this Act, the Di-
17 rector of the Cybersecurity and Infrastructure Secu-
18 rity Agency of the Department of Homeland Secu-
19 rity shall submit to the Committee on Homeland Se-
20 curity of the House of Representatives and the Com-
21 mittee on Homeland Security and Governmental Af-
22 fairs of the Senate a report describing how the
23 Cyber Incident Review Office of the Department of
24 Homeland Security (established pursuant to section
25 2220A of the Homeland Security Act of 2002, as

1 added by subsection (a)) has carried out activities
2 under subsection (c)(6) of such section 2220A by
3 proactively identifying opportunities to use cyberse-
4 curity incident data to inform and enable cybersecu-
5 rity research carried out by academic institutions
6 and other private sector organizations.

7 (c) TITLE XXII TECHNICAL AND CLERICAL AMEND-
8 MENTS.—

9 (1) TECHNICAL AMENDMENTS.—

10 (A) HOMELAND SECURITY ACT OF 2002.—

11 Subtitle A of title XXII of the Homeland Secu-
12 rity Act of 2002 (6 U.S.C. 651 et seq.) is
13 amended—

14 (i) in section 2202 (6 U.S.C. 652)—

15 (I) in paragraph (11), by striking
16 “and” after the semicolon;

17 (II) in the first paragraph (12)
18 (relating to appointment of a Cyberse-
19 curity State Coordinator) by striking
20 “as described in section 2215; and”
21 and inserting “as described in section
22 2217;”;

23 (III) by redesignating the second
24 paragraph (12) (relating to the .gov

1 internet domain) as paragraph (13);

2 and

3 (IV) by redesignating the third
4 paragraph (12) (relating to carrying
5 out such other duties and responsibil-
6 ities) as paragraph (14);

7 (ii) in the first section 2215 (6 U.S.C.
8 665; relating to the duties and authorities
9 relating to .gov internet domain), by
10 amending the section enumerator and
11 heading to read as follows:

12 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**
13 **INTERNET DOMAIN.”;**

14 (iii) in the second section 2215 (6
15 U.S.C. 665b; relating to the joint cyber
16 planning office), by amending the section
17 enumerator and heading to read as follows:

18 **“SEC. 2216. JOINT CYBER PLANNING OFFICE.”;**

19 (iv) in the third section 2215 (6
20 U.S.C. 665c; relating to the Cybersecurity
21 State Coordinator), by amending the sec-
22 tion enumerator and heading to read as
23 follows:

1 **“SEC. 2217. CYBERSECURITY STATE COORDINATOR.”;**

2 (v) in the fourth section 2215 (6
3 U.S.C. 665d; relating to Sector Risk Man-
4 agement Agencies), by amending the sec-
5 tion enumerator and heading to read as
6 follows:

7 **“SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.”;**

8 (vi) in section 2216 (6 U.S.C. 665e;
9 relating to the Cybersecurity Advisory
10 Committee), by amending the section enu-
11 merator and heading to read as follows:

12 **“SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.”; and**

13 (vii) in section 2217 (6 U.S.C. 665f;
14 relating to Cybersecurity Education and
15 Training Programs), by amending the sec-
16 tion enumerator and heading to read as
17 follows:

18 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**
19 **PROGRAMS.”.**

20 (B) CONSOLIDATED APPROPRIATIONS ACT,
21 2021.—Paragraph (1) of section 904(b) of divi-
22 sion U of the Consolidated Appropriations Act,
23 2021 (Public Law 116–260) is amended, in the
24 matter preceding subparagraph (A), by insert-
25 ing “of 2002” after “Homeland Security Act”.

1 (2) CLERICAL AMENDMENT.—The table of con-
2 tents in section 1(b) of the Homeland Security Act
3 of 2002 is amended by striking the items relating to
4 sections 2214 through 2217 and inserting the fol-
5 lowing new items:

“Sec. 2214. National Asset Database.

“Sec. 2215. Duties and authorities relating to .gov internet domain.

“Sec. 2216. Joint cyber planning office.

“Sec. 2217. Cybersecurity State Coordinator.

“Sec. 2218. Sector Risk Management Agencies.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity Education and Training Programs.

“Sec. 2220A. Cyber Incident Review Office.”.