

.....
(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 into information technology hardware, soft-
19 ware, operating systems, peripherals (such as infor-
20 mation technology products), or services at any point
21 during the life cycle in order to infiltrate the net-
22 works of third parties where such products, services,
23 or technologies are deployed.

24 “(b) CYBER INCIDENT REVIEW OFFICE.—There is
25 established in the Agency a Cyber Incident Review Office

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

8 “(c) ACTIVITIES.—The Office shall, in furtherance of
9 the activities specified in sections 2202(e), 2209(c), and
10 2203—

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

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

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

1 dents that together satisfy such definition, conduct
2 a review of the details surrounding such covered cy-
3 bersecurity incident or group of such incidents and
4 identify ways to prevent or mitigate similar incidents
5 in the future;

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

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

19 “(6) leverage information gathered regarding
20 cybersecurity incidents to enhance the quality and
21 effectiveness of bi-directional information sharing
22 and coordination efforts with appropriate stake-
23 holders, including sector coordinating councils, infor-
24 mation sharing and analysis organizations, tech-
25 nology providers, cybersecurity and incident response

1 firms, and security researchers, including by estab-
2 lishing mechanisms to receive feedback from such
3 stakeholders regarding how the Agency can most ef-
4 fectively support private sector cybersecurity; and

5 “(6) proactively identify opportunities, in ac-
6 cordance with the protections specified in sub-
7 sections (e) and (f), to leverage and utilize data on
8 cybersecurity incidents in a manner that enables and
9 strengthens cybersecurity research carried out by
10 academic institutions and other private sector orga-
11 nizations, to the greatest extent practicable.

12 “(d) COVERED CYBERSECURITY INCIDENT REPORT-
13 ING REQUIREMENTS AND PROCEDURES.—

14 “(1) IN GENERAL.—Not later than 270 days
15 after the date of the enactment of this section, the
16 Director, in consultation with Sector Risk Manage-
17 ment Agencies and the heads of other Federal de-
18 partments and agencies, as appropriate, shall, after
19 a 60 day consultative period, followed by a 90 day
20 comment period with appropriate stakeholders, in-
21 cluding sector coordinating councils, publish in the
22 Federal Register an interim final rule implementing
23 this section. Notwithstanding section 553 of title 5,
24 United States Code, such rule shall be effective, on
25 an interim basis, immediately upon publication, but

1 may be subject to change and revision after public
2 notice and opportunity for comment. The Director
3 shall issue a final rule not later than one year after
4 publication of such interim final rule. Such interim
5 final rule shall—

6 “(A) require covered entities to submit to
7 the Office reports containing information relat-
8 ing to covered cybersecurity incidents; and

9 “(B) establish procedures that clearly de-
10 scribe—

11 “(i) the types of critical infrastructure
12 entities determined to be covered entities;

13 “(ii) the types of cybersecurity inci-
14 dents determined to be covered cybersecu-
15 rity incidents;

16 “(iii) the mechanisms by which cov-
17 ered cybersecurity incident reports under
18 subparagraph (A) are to be submitted, in-
19 cluding—

20 “(I) the contents, described in
21 paragraph (4), to be included in each
22 such report, including any supple-
23 mental reporting requirements;

1 “(II) the timing relating to when
2 each such report should be submitted;
3 and

4 “(III) the format of each such re-
5 port;

6 “(iv) describe the manner in which
7 the Office will carry out enforcement ac-
8 tions under subsection (g), including with
9 respect to the issuance of subpoenas, con-
10 ducting examinations, and other aspects
11 relating to noncompliance; and

12 “(v) any other responsibilities to be
13 carried out by covered entities, or other
14 procedures necessary to implement this
15 section.

16 “(2) COVERED ENTITIES.—In determining
17 which types of critical infrastructure entities are cov-
18 ered entities for purposes of this section, the Sec-
19 retary, acting through the Director, in consultation
20 with Sector Risk Management Agencies and the
21 heads of other Federal departments and agencies, as
22 appropriate, shall consider—

23 “(A) the consequences that disruption to
24 or compromise of such an entity could cause to

1 national security, economic security, or public
2 health and safety;

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

6 “(C) the extent to which damage, disrup-
7 tion, or unauthorized access to such an entity
8 will disrupt the reliable operation of other crit-
9 ical infrastructure assets; and

10 “(D) the extent to which an entity or sec-
11 tor is subject to existing regulatory require-
12 ments to report cybersecurity incidents, and the
13 possibility of coordination and sharing of re-
14 ports between the Office and the regulatory au-
15 thority to which such entity submits such other
16 reports.

17 “(3) OUTREACH TO COVERED ENTITIES.—

18 “(A) IN GENERAL.—The Director shall
19 conduct an outreach and education campaign to
20 inform covered entities of the requirements of
21 this section.

22 “(B) ELEMENTS.—The outreach and edu-
23 cation campaign under subparagraph (A) shall
24 include the following:

1 “(i) Overview of the interim final rule
2 and final rule issued pursuant to this sec-
3 tion.

4 “(ii) Overview of reporting require-
5 ments and procedures issued pursuant to
6 paragraph (1).

7 “(iii) Overview of mechanisms to sub-
8 mit to the Office covered cybersecurity in-
9 cident reports and information relating to
10 the disclosure, retention, and use of inci-
11 dent reports under this section.

12 “(iv) Overview of the protections af-
13 farded to covered entities for complying
14 with requirements under subsection (f).

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

19 “(C) COORDINATION.—The Director may
20 conduct the outreach and education campaign
21 under subparagraph (A) through coordination
22 with the following:

23 “(i) The Critical Infrastructure Part-
24 nership Advisory Council established pur-
25 suant to section 871.

1 “(ii) Information Sharing and Anal-
2 ysis Organizations.

3 “(iii) Any other means the Director
4 determines to be effective to conduct such
5 campaign.

6 “(4) COVERED CYBERSECURITY INCIDENTS.—

7 “(A) CONSIDERATIONS.—In accordance
8 with subparagraph (B), in determining which
9 types of incidents are covered cybersecurity in-
10 cidents for purposes of this section, the Direc-
11 tor shall consider—

12 “(i) the sophistication or novelty of
13 the tactics used to perpetrate such an inci-
14 dent, as well as the type, volume, and sen-
15 sitivity 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 con-
21 trol and data acquisition systems, distrib-
22 uted control systems, and programmable
23 logic controllers.

24 “(B) MINIMUM THRESHOLDS.—For a cy-
25 bersecurity incident to be considered a covered

1 cybersecurity incident a cybersecurity incident
2 shall, at a minimum, include at least one of the
3 following:

4 “(i) Unauthorized access to an infor-
5 mation system or network that leads to
6 loss of confidentiality, integrity, or avail-
7 ability of such information system or net-
8 work, or has a serious impact on the safety
9 and resiliency of operational systems and
10 processes.

11 “(ii) Disruption of business or indus-
12 trial operations due to a denial of service
13 attack, a ransomware attack, or exploi-
14 tation of a zero-day vulnerability,
15 against—

16 “(I) an information system or
17 network; or

18 “(II) an operational technology
19 system or process.

20 “(iii) Unauthorized access or disrup-
21 tion of business or industrial operations
22 due to loss of service facilitated through,
23 or caused by a compromise of, a cloud
24 service provider, managed service provider,

1 other third-party data hosting provider, or
2 supply chain attack.

3 “(5) REPORTS.—

4 “(A) TIMING.—

5 “(i) IN GENERAL.—The Director, in
6 consultation with Sector Risk Management
7 Agencies and the heads of other Federal
8 departments and agencies, as appropriate,
9 shall establish reporting timelines for cov-
10 ered entities to submit promptly to the Of-
11 fice covered cybersecurity incident reports,
12 as the Director determines reasonable and
13 appropriate based on relevant factors, such
14 as the nature, severity, and complexity of
15 the covered cybersecurity incident at issue
16 and the time required for investigation, but
17 in no case may the Director require report-
18 ing by a covered entity earlier than 72
19 hours after confirmation that a covered cy-
20 bersecurity incident has occurred.

21 “(ii) CONSIDERATIONS.—In deter-
22 mining reporting timelines under clause
23 (i), the Director shall—

24 “(I) consider any existing regu-
25 latory reporting requirements, similar

1 in scope purpose, and timing to the
2 reporting requirements under this sec-
3 tion, to which a covered entity may
4 also be subject, and make efforts to
5 harmonize the timing and contents of
6 any such reports to the maximum ex-
7 tent practicable; and

8 “(II) balance the Agency’s need
9 for situational awareness with a cov-
10 ered entity’s ability to conduct inci-
11 dent response and investigations.

12 “(B) THIRD PARTY REPORTING.—

13 “(i) IN GENERAL.—A covered entity
14 may submit a covered cybersecurity inci-
15 dent report through a third party entity or
16 Information Sharing and Analysis Organi-
17 zation.

18 “(ii) DUTY TO ENSURE COMPLI-
19 ANCE.—Third party reporting under this
20 subparagraph does not relieve a covered
21 entity of the duty to ensure compliance
22 with the requirements of this paragraph.

23 “(C) SUPPLEMENTAL REPORTING.—A cov-
24 ered entity shall submit promptly to the Office,
25 until such date that such covered entity notifies

1 the Office that the cybersecurity incident inves-
2 tigation at issue has concluded and the associ-
3 ated covered cybersecurity incident has been
4 fully mitigated and resolved, periodic updates or
5 supplements to a previously submitted covered
6 cybersecurity incident report if new or different
7 information becomes available that would other-
8 wise have been required to have been included
9 in such previously submitted report. In deter-
10 mining reporting timelines, the Director may
11 choose to establish a flexible, phased reporting
12 timeline for covered entities to report informa-
13 tion in a manner that aligns with investigative
14 timelines and allows covered entities to
15 prioritize incident response efforts over compli-
16 ance.

17 “(D) CONTENTS.—Covered cybersecurity
18 incident reports submitted pursuant to this sec-
19 tion shall contain such information as the Di-
20 rector prescribes, including the following infor-
21 mation, to the extent applicable and available,
22 with respect to a covered cybersecurity incident:

23 “(i) A description of the covered cy-
24 bersecurity incident, including identifica-
25 tion of the affected information systems,

1 networks, or devices that were, or are rea-
2 sonably believed to have been, affected by
3 such incident, and the estimated date
4 range of such incident.

5 “(ii) Where applicable, a description
6 of the vulnerabilities exploited and the se-
7 curity defenses that were in place, as well
8 as the tactics, techniques, and procedures
9 relevant to such incident.

10 “(iii) Where applicable, any identi-
11 fying information related to the actor rea-
12 sonably believed to be responsible for such
13 incident.

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

19 “(v) Contact information, such as
20 telephone number or electronic mail ad-
21 dress, that the Office may use to contact
22 the covered entity or, where applicable, an
23 authorized agent of such covered entity, or,
24 where applicable, the service provider, act-
25 ing with the express permission, and at the

1 direction, of such covered entity, to assist
2 with compliance with the requirements of
3 this section.

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

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

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

23 “(B) coordinate with other regulatory au-
24 thorities that receive reports relating to cyberse-
25 curity incidents to identify opportunities to

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

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

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

19 “(A) a cybersecurity purpose;

20 “(B) the purpose of identifying—

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

23 “(ii) a security vulnerability;

1 “(C) the purpose of responding to, or oth-
2 erwise preventing, or mitigating a specific
3 threat of—

4 “(i) death;

5 “(ii) serious bodily harm; or

6 “(iii) serious economic harm, includ-
7 ing a terrorist act or a use of a weapon of
8 mass destruction;

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

14 “(E) the purpose of preventing, inves-
15 tigating, disrupting, or prosecuting an offense
16 related to a threat—

17 “(i) described in subparagraphs (B)
18 through (D); or

19 “(ii) specified in section
20 105(d)(5)(A)(v) of the Cybersecurity Act
21 of 2015 (enacted as division N of the Con-
22 solidated Appropriations Act, 2016 (Public
23 Law 114–113; 6 U.S.C.
24 1504(d)(5)(A)(v))).

25 “(2) EXCEPTIONS.—

1 “(A) RAPID, CONFIDENTIAL, BI-DIREC-
2 TIONAL SHARING OF CYBER THREAT INDICA-
3 TORS.—Upon receiving a covered cybersecurity
4 incident report submitted pursuant to this sec-
5 tion, the Office shall immediately review such
6 report to determine whether the incident that is
7 the subject of such report is connected to an
8 ongoing cybersecurity threat or security vulner-
9 ability and where applicable, use such report to
10 identify, develop, and rapidly disseminate to ap-
11 propriate stakeholders actionable, anonymized
12 cyber threat indicators and defensive measures.

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

23 “(3) PRIVACY AND CIVIL LIBERTIES.—Informa-
24 tion contained in reports submitted to the Office
25 pursuant to subsections (d) and (h) shall be re-

1 tained, used, and disseminated, where permissible
2 and appropriate, by the Federal Government in a
3 manner consistent with processes for the protection
4 of personal information adopted pursuant to section
5 105 of the Cybersecurity Act of 2015 (enacted as di-
6 vision N of the Consolidated Appropriations Act,
7 2016 (Public Law 114–113; 6 U.S.C. 1504)).

8 “(4) PROHIBITION ON USE OF INFORMATION IN
9 REGULATORY ACTIONS.—

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

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

1 “(f) PROTECTIONS FOR REPORTING ENTITIES AND
2 INFORMATION.—Reports describing covered cybersecurity
3 incidents submitted to the Office by covered entities in ac-
4 cordance with subsection (d), as well as voluntarily-sub-
5 mitted cybersecurity incident reports submitted to the Of-
6 fice pursuant to subsection (h), shall be—

7 “(1) entitled to the protections against liability
8 described in section 106 of the Cybersecurity Act of
9 2015 (enacted as division N of the Consolidated Ap-
10 propriations Act, 2016 (Public Law 114–113; 6
11 U.S.C. 1505));

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

18 “(3) considered the commercial, financial, and
19 proprietary information of the covered entity when
20 so designated by the covered entity.

21 “(g) NONCOMPLIANCE WITH REQUIRED REPORT-
22 ING.—

23 “(1) PURPOSE.—In the event a covered entity
24 experiences a cybersecurity incident but does not
25 comply with the reporting requirements under this

1 section, the Director may obtain information about
2 such incident by engaging directly such covered enti-
3 ty in accordance with paragraph (2) to request in-
4 formation about such incident, or, if the Director is
5 unable to obtain such information through such en-
6 gagement, by issuing a subpoena to such covered en-
7 tity, subject to paragraph (3), to gather information
8 sufficient to determine whether such incident is a
9 covered cybersecurity incident, and if so, whether ad-
10 ditional action is warranted pursuant to paragraph
11 (4).

12 “(2) INITIAL REQUEST FOR INFORMATION.—

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

1 tion into the details surrounding such incident
2 are warranted pursuant to paragraph (4).

3 “(B) TREATMENT.—Information provided
4 to the Office in response to a request under
5 subparagraph (A) shall be treated as if such in-
6 formation was submitted pursuant to the re-
7 porting procedures established in accordance
8 with subsection (d).

9 “(3) AUTHORITY TO ISSUE SUBPOENAS.—

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

1 mation as is necessary to carry out activities
2 described in subsection (c).

3 “(B) CIVIL ACTION.—If a covered entity
4 does not comply with a subpoena, the Director
5 may bring a civil action in a district court of
6 the United States to enforce such subpoena. An
7 action under this paragraph may be brought in
8 the judicial district in which the entity against
9 which the action is brought resides, is found, or
10 does business. The court may punish a failure
11 to obey an order of the court to comply with the
12 subpoena as a contempt of court.

13 “(C) NON-APPLICABILITY OF PROTEC-
14 TIONS.—The protections described in subsection
15 (f) do not apply to a covered entity that is the
16 recipient of a subpoena under this paragraph
17 (3).

18 “(4) ADDITIONAL ACTIONS.—

19 “(A) EXAMINATION.—If, based on the in-
20 formation provided in response to a subpoena
21 issued pursuant to paragraph (3), the Director
22 determines that the cybersecurity incident at
23 issue is a significant cyber incident, or is part
24 of a group of related cybersecurity incidents
25 that together satisfy the definition of a signifi-

1 cant cyber incident, and a more thorough exam-
2 ination of the details surrounding such incident
3 is warranted in order to carry out activities de-
4 scribed in subsection (c), the Director may di-
5 rect the Office to conduct an examination of
6 such incident in order to enhance the Agency’s
7 situational awareness of cybersecurity threats
8 across critical infrastructure sectors, in a man-
9 ner consistent with privacy and civil liberties
10 protections under applicable law.

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

1 “(h) VOLUNTARY REPORTING OF CYBER INCI-
2 DENTS.—The Agency shall receive cybersecurity incident
3 reports submitted voluntarily by entities that are not cov-
4 ered entities, or concerning cybersecurity incidents that do
5 not satisfy the definition of covered cybersecurity incidents
6 but may nevertheless enhance the Agency’s situational
7 awareness of cybersecurity threats across critical infra-
8 structure sectors. The protections under this section appli-
9 cable to covered cybersecurity incident reports shall apply
10 in the same manner and to the same extent to voluntarily-
11 submitted cybersecurity incident reports under this sub-
12 section.

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

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

4 “(k) SAVING PROVISION.—Nothing in this section
5 may be construed as modifying, superseding, or otherwise
6 affecting in any manner any regulatory authority held by
7 a Federal department or agency, including Sector Risk
8 Management Agencies, existing on the day before the date
9 of the enactment of this section, or any existing regulatory
10 requirements or obligations that apply to covered enti-
11 ties.”.

12 (b) REPORTS.—

13 (1) ON STAKEHOLDER ENGAGEMENT.—Not
14 later than 30 days before the date on which that the
15 Director of the Cybersecurity and Infrastructure Se-
16 curity Agency of the Department of Homeland Secu-
17 rity intends to issue an interim final rule under sub-
18 section (d)(1) of section 2220A of the Homeland Se-
19 curity Act of 2002 (as added by subsection (a)), the
20 Director shall submit to the Committee on Home-
21 land Security of the House of Representatives and
22 the Committee on Homeland Security and Govern-
23 mental Affairs of the Senate a report that describes
24 how the Director engaged stakeholders in the devel-
25 opment of such interim final rules.

1 (2) ON OPPORTUNITIES TO STRENGTHEN CY-
2 BERSECURITY RESEARCH.—Not later than one year
3 after the date of the enactment of this Act, the Di-
4 rector of the Cybersecurity and Infrastructure Secu-
5 rity Agency of the Department of Homeland Secu-
6 rity shall submit to the Committee on Homeland Se-
7 curity of the House of Representatives and the Com-
8 mittee on Homeland Security and Governmental Af-
9 fairs of the Senate a report describing how the
10 Cyber Incident Review Office of the Department of
11 Homeland Security (established pursuant to section
12 2220A of the Homeland Security Act of 2002, as
13 added by subsection (a)) has carried out activities
14 under subsection (c)(6) of such section 2220A by
15 proactively identifying opportunities to use cyberse-
16 curity incident data to inform and enable cybersecu-
17 rity research carried out by academic institutions
18 and other private sector organizations.

19 (c) TITLE XXII TECHNICAL AND CLERICAL AMEND-
20 MENTS.—

21 (1) TECHNICAL AMENDMENTS.—

22 (A) HOMELAND SECURITY ACT OF 2002.—
23 Subtitle A of title XXII of the Homeland Secu-
24 rity Act of 2002 (6 U.S.C. 651 et seq.) is
25 amended—

1 (i) in section 2202 (6 U.S.C. 652)—

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

4 (II) in the first paragraph (12)
5 (relating to appointment of a Cyberse-
6 curity State Coordinator) by striking
7 “as described in section 2215; and”
8 and inserting “as described in section
9 2217;”;

10 (III) by redesignating the second
11 paragraph (12) (relating to the .gov
12 internet domain) as paragraph (13);
13 and

14 (IV) by redesignating the third
15 paragraph (12) (relating to carrying
16 out such other duties and responsibil-
17 ities) as paragraph (14);

18 (ii) in the first section 2215 (6 U.S.C.
19 665; relating to the duties and authorities
20 relating to .gov internet domain), by
21 amending the section enumerator and
22 heading to read as follows:

1 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**
2 **INTERNET DOMAIN.”;**

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

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

8 (iv) in the third section 2215 (6
9 U.S.C. 665c; relating to the Cybersecurity
10 State Coordinator), by amending the sec-
11 tion enumerator and heading to read as
12 follows:

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

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

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

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

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

25 (vii) in section 2217 (6 U.S.C. 665f;
26 relating to Cybersecurity Education and

1 Training Programs), by amending the sec-
2 tion enumerator and heading to read as
3 follows:

4 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**
5 **PROGRAMS.”.**

6 (B) CONSOLIDATED APPROPRIATIONS ACT,
7 2021.—Paragraph (1) of section 904(b) of divi-
8 sion U of the Consolidated Appropriations Act,
9 2021 (Public Law 116–260) is amended, in the
10 matter preceding subparagraph (A), by insert-
11 ing “of 2002” after “Homeland Security Act”.

12 (2) CLERICAL AMENDMENT.—The table of con-
13 tents in section 1(b) of the Homeland Security Act
14 of 2002 is amended by striking the items relating to
15 sections 2214 through 2217 and inserting the fol-
16 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.”.