

AMENDMENT TO RULES COMM. PRINT 117-13

OFFERED BY M s. Clarke

Add at the end of subtitle D of title XV of division
A the following:

1 **SEC. 15** . **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).

1 “(3) COVERED CYBSECURITY INCIDENT.—The
2 term ‘covered cybersecurity incident’ means a cyber-
3 security incident experienced by a covered entity
4 that satisfies the definition and criteria established
5 by the Director in the reporting requirements and
6 procedures issued pursuant to subsection (d).

7 “(4) CYBER THREAT INDICATOR.—The term
8 ‘cyber threat indicator’ has the meaning given such
9 term in section 102 of the Cybersecurity Act of 2015
10 (enacted as division N of the Consolidated Appro-
11 priations Act, 2016 (Public Law 114–113; 6 U.S.C.
12 1501)).

13 “(5) CYBERSECURITY PURPOSE.—The term ‘cy-
14 bersecurity purpose’ has the meaning given such
15 term in section 102 of the Cybersecurity Act of 2015
16 (enacted as division N of the Consolidated Appro-
17 priations Act, 2016 (Public Law 114–113; 6 U.S.C.
18 1501)).

19 “(6) CYBERSECURITY THREAT.—The term ‘cy-
20 bersecurity threat’ has the meaning given such term
21 in section 102 of the Cybersecurity Act of 2015 (en-
22 acted as division N of the Consolidated Appropria-
23 tions Act, 2016 (Public Law 114–113; 6 U.S.C.
24 1501)).

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

7 “(8) INFORMATION SHARING AND ANALYSIS OR-
8 GANIZATION.—The term ‘Information Sharing and
9 Analysis Organization’ has the meaning given such
10 term in section 2222(5).

11 “(9) INFORMATION SYSTEM.—The term ‘infor-
12 mation system’ has the meaning given such term in
13 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(9)).

17 “(10) INTELLIGENCE COMMUNITY.—The term
18 ‘intelligence community’ has the meaning given the
19 term in section 3(4) of the National Security Act of
20 1947 (50 U.S.C. 3003(4)).

21 “(11) MANAGED SERVICE PROVIDER.—The
22 term ‘managed service provider’ means an entity
23 that delivers services, such as network, application,
24 infrastructure, or security services, via ongoing and
25 regular support and active administration on cus-

1 tomers’ premises, in the managed service provider’s
2 data center (such as hosting), or in a third-party
3 data center.

4 “(12) SECURITY CONTROL.—The term ‘security
5 control’ has the meaning given such term in section
6 102 of the Cybersecurity Act of 2015 (enacted as di-
7 vision N of the Consolidated Appropriations Act,
8 2016 (Public Law 114–113; 6 U.S.C. 1501)).

9 “(13) SECURITY VULNERABILITY.—The term
10 ‘security vulnerability’ has the meaning given such
11 term in section 102 of the Cybersecurity Act of 2015
12 (enacted as division N of the Consolidated Appro-
13 priations Act, 2016 (Public Law 114–113; 6 U.S.C.
14 1501)).

15 “(14) SIGNIFICANT CYBER INCIDENT.—The
16 term ‘significant cyber incident’ means a cyber inci-
17 dent, or a group of related cyber incidents, that the
18 Director determines is likely to result in demon-
19 strable harm to the national security interests, for-
20 eign relations, or economy of the United States or
21 to the public confidence, civil liberties, or public
22 health and safety of the American people.

23 “(15) SUPPLY CHAIN ATTACK.—The term ‘sup-
24 ply chain attack’ means an attack that allows an ad-
25 versary to utilize implants or other vulnerabilities in-

1 serted into information technology hardware, soft-
2 ware, operating systems, peripherals (such as infor-
3 mation technology products), or services at any point
4 during the life cycle in order to infiltrate the net-
5 works of third parties where such products, services,
6 or technologies are deployed.

7 “(b) CYBER INCIDENT REVIEW OFFICE.—There is
8 established in the Agency a Cyber Incident Review Office
9 (in this section referred to as the ‘Office’) to receive, ag-
10 gregate, and analyze reports related to covered cybersecu-
11 rity incidents submitted by covered entities in furtherance
12 of the activities specified in subsection (c) of this section
13 and sections 2202(e), 2209(c), and 2203 to enhance the
14 situational awareness of cybersecurity threats across crit-
15 ical infrastructure sectors.

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

19 “(1) receive, aggregate, analyze, and secure re-
20 ports from covered entities related to a covered cy-
21 bersecurity incident to assess the effectiveness of se-
22 curity controls and identify tactics, techniques, and
23 procedures adversaries use to overcome such con-
24 trols;

1 “(2) facilitate the timely sharing between rel-
2 evant critical infrastructure owners and operators
3 and, as appropriate, the intelligence community of
4 information relating to covered cybersecurity inci-
5 dents, particularly with respect to an ongoing cyber-
6 security threat or security vulnerability;

7 “(3) for a covered cybersecurity incident that
8 also satisfies the definition of a significant cyber in-
9 cident, or are part of a group of related cyber inci-
10 dents that together satisfy such definition, conduct
11 a review of the details surrounding such covered cy-
12 bersecurity incident or group of such incidents and
13 identify ways to prevent or mitigate similar incidents
14 in the future;

15 “(4) with respect to covered cybersecurity inci-
16 dent reports under subsection (d) involving an ongo-
17 ing cybersecurity threat or security vulnerability, im-
18 mediately review such reports for cyber threat indi-
19 cators that can be anonymized and disseminated,
20 with defensive measures, to appropriate stake-
21 holders, in coordination with other Divisions within
22 the Agency, as appropriate;

23 “(5) publish quarterly unclassified, public re-
24 ports that describe aggregated, anonymized observa-
25 tions, findings, and recommendations based on cov-

1 ered cybersecurity incident reports under subsection
2 (d);

3 “(6) leverage information gathered regarding
4 cybersecurity incidents to enhance the quality and
5 effectiveness of bi-directional information sharing
6 and coordination efforts with appropriate stake-
7 holders, including sector coordinating councils, infor-
8 mation sharing and analysis organizations, tech-
9 nology providers, cybersecurity and incident response
10 firms, and security researchers, including by estab-
11 lishing mechanisms to receive feedback from such
12 stakeholders regarding how the Agency can most ef-
13 fectively support private sector cybersecurity; and

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

21 “(d) COVERED CYBERSECURITY INCIDENT REPORT-
22 ING REQUIREMENTS AND PROCEDURES.—

23 “(1) IN GENERAL.—Not later than 270 days
24 after the date of the enactment of this section, the
25 Director, in consultation with Sector Risk Manage-

1 ment Agencies and the heads of other Federal de-
2 partments and agencies, as appropriate, shall, after
3 a 60 day consultative period, followed by a 90 day
4 comment period with appropriate stakeholders, in-
5 cluding sector coordinating councils, publish in the
6 Federal Register an interim final rule implementing
7 this section. Notwithstanding section 553 of title 5,
8 United States Code, such rule shall be effective, on
9 an interim basis, immediately upon publication, but
10 may be subject to change and revision after public
11 notice and opportunity for comment. The Director
12 shall issue a final rule not later than one year after
13 publication of such interim final rule. Such interim
14 final rule shall—

15 “(A) require covered entities to submit to
16 the Office reports containing information relat-
17 ing to covered cybersecurity incidents; and

18 “(B) establish procedures that clearly de-
19 scribe—

20 “(i) the types of critical infrastructure
21 entities determined to be covered entities;

22 “(ii) the types of cybersecurity inci-
23 dents determined to be covered cybersecu-
24 rity incidents;

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

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

9 “(II) the timing relating to when
10 each such report should be submitted;
11 and

12 “(III) the format of each such re-
13 port;

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

20 “(v) any other responsibilities to be
21 carried out by covered entities, or other
22 procedures necessary to implement this
23 section.

24 “(2) COVERED ENTITIES.—In determining
25 which types of critical infrastructure entities are cov-

1 ered entities for purposes of this section, the Sec-
2 retary, acting through the Director, in consultation
3 with Sector Risk Management Agencies and the
4 heads of other Federal departments and agencies, as
5 appropriate, shall consider—

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

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

13 “(C) the extent to which damage, disrup-
14 tion, or unauthorized access to such and entity
15 will disrupt the reliable operation of other crit-
16 ical infrastructure assets; and

17 “(D) the extent to which an entity or sec-
18 tor is subject to existing regulatory require-
19 ments to report cybersecurity incidents, and the
20 possibility of coordination and sharing of re-
21 ports between the Office and the regulatory au-
22 thority to which such entity submits such other
23 reports.

24 “(3) OUTREACH TO COVERED ENTITIES.—

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

5 “(B) ELEMENTS.—The outreach and edu-
6 cation campaign under subparagraph (A) shall
7 include the following:

8 “(i) Overview of the interim final rule
9 and final rule issued pursuant to this sec-
10 tion.

11 “(ii) Overview of reporting require-
12 ments and procedures issued pursuant to
13 paragraph (1).

14 “(iii) Overview of mechanisms to sub-
15 mit to the Office covered cybersecurity in-
16 cident reports and information relating to
17 the disclosure, retention, and use of inci-
18 dent reports under this section.

19 “(iv) Overview of the protections af-
20 forded to covered entities for complying
21 with requirements under subsection (f).

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

1 “(C) COORDINATION.—The Director may
2 conduct the outreach and education campaign
3 under subparagraph (A) through coordination
4 with the following:

5 “(i) The Critical Infrastructure Part-
6 nership Advisory Council established pur-
7 suant to section 871.

8 “(ii) Information Sharing and Anal-
9 ysis Organizations.

10 “(iii) Any other means the Director
11 determines to be effective to conduct such
12 campaign.

13 “(4) COVERED CYBERSECURITY INCIDENTS.—

14 “(A) CONSIDERATIONS.—In accordance
15 with subparagraph (B), in determining which
16 types of incidents are covered cybersecurity in-
17 cidents for purposes of this section, the Direc-
18 tor shall consider—

19 “(i) the sophistication or novelty of
20 the tactics used to perpetrate such an inci-
21 dent, as well as the type, volume, and sen-
22 sitivity of the data at issue;

23 “(ii) the number of individuals di-
24 rectly or indirectly affected or potentially
25 affected by such an incident; and

1 “(iii) potential impacts on industrial
2 control systems, such as supervisory con-
3 trol and data acquisition systems, distrib-
4 uted control systems, and programmable
5 logic controllers.

6 “(B) MINIMUM THRESHOLDS.—For a cy-
7 bersecurity incident to be considered a covered
8 cybersecurity incident a cybersecurity incident
9 shall, at a minimum, include at least one of the
10 following:

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

18 “(ii) Disruption of business or indus-
19 trial operations due to a denial of service
20 attack, a ransomware attack, or exploi-
21 tation of a zero-day vulnerability,
22 against—

23 “(I) an information system or
24 network; or

1 “(II) an operational technology
2 system or process.

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

10 “(5) REPORTS.—

11 “(A) TIMING.—

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

1 hours after confirmation that a covered cy-
2 bersecurity incident has occurred.

3 “(ii) CONSIDERATIONS.—In deter-
4 mining reporting timelines under clause
5 (i), the Director shall—

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

15 “(II) balance the Agency’s need
16 for situational awareness with a cov-
17 ered entity’s ability to conduct inci-
18 dent response and investigations.

19 “(B) THIRD PARTY REPORTING.—

20 “(i) IN GENERAL.—A covered entity
21 may submit a covered cybersecurity inci-
22 dent report through a third party entity or
23 Information Sharing and Analysis Organi-
24 zation.

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

6 “(C) SUPPLEMENTAL REPORTING.—A cov-
7 ered entity shall submit promptly to the Office,
8 until such date that such covered entity notifies
9 the Office that the cybersecurity incident inves-
10 tigation at issue has concluded and the associ-
11 ated covered cybersecurity incident has been
12 fully mitigated and resolved, periodic updates or
13 supplements to a previously submitted covered
14 cybersecurity incident report if new or different
15 information becomes available that would other-
16 wise have been required to have been included
17 in such previously submitted report. In deter-
18 mining reporting timelines, the Director may
19 choose to establish a flexible, phased reporting
20 timeline for covered entities to report informa-
21 tion in a manner that aligns with investigative
22 timelines and allows covered entities to
23 prioritize incident response efforts over compli-
24 ance.

1 “(D) CONTENTS.—Covered cybersecurity
2 incident reports submitted pursuant to this sec-
3 tion shall contain such information as the Di-
4 rector prescribes, including the following infor-
5 mation, to the extent applicable and available,
6 with respect to a covered cybersecurity incident:

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

14 “(ii) Where applicable, a description
15 of the vulnerabilities exploited and the se-
16 curity defenses that were in place, as well
17 as the tactics, techniques, and procedures
18 relevant to such incident.

19 “(iii) Where applicable, any identi-
20 fying information related to the actor rea-
21 sonably believed to be responsible for such
22 incident.

23 “(iv) Where applicable, identification
24 of the category or categories of information
25 that was, or is reasonably believed to have

1 been, accessed or acquired by an unauthor-
2 ized person.

3 “(v) Contact information, such as
4 telephone number or electronic mail ad-
5 dress, that the Office may use to contact
6 the covered entity or, where applicable, an
7 authorized agent of such covered entity, or,
8 where applicable, the service provider, act-
9 ing with the express permission, and at the
10 direction, of such covered entity, to assist
11 with compliance with the requirements of
12 this section.

13 “(6) RESPONSIBILITIES OF COVERED ENTI-
14 TIES.—Covered entities that experience a covered cy-
15 bersecurity incident shall coordinate with the Office
16 to the extent necessary to comply with this section,
17 and, to the extent practicable, cooperate with the Of-
18 fice in a manner that supports enhancing the Agen-
19 cy’s situational awareness of cybersecurity threats
20 across critical infrastructure sectors.

21 “(7) HARMONIZING REPORTING REQUIRE-
22 MENTS.—In establishing the reporting requirements
23 and procedures under paragraph (1), the Director
24 shall, to the maximum extent practicable—

1 “(A) review existing regulatory require-
2 ments, including the information required in
3 such reports, to report cybersecurity incidents
4 that may apply to covered entities, and ensure
5 that any such reporting requirements and pro-
6 cedures avoid conflicting, duplicative, or bur-
7 densome requirements; and

8 “(B) coordinate with other regulatory au-
9 thorities that receive reports relating to cyberse-
10 curity incidents to identify opportunities to
11 streamline reporting processes, and where fea-
12 sible, enter into agreements with such authori-
13 ties to permit the sharing of such reports with
14 the Office, consistent with applicable law and
15 policy, without impacting the Office’s ability to
16 gain timely situational awareness of a covered
17 cybersecurity incident or significant cyber inci-
18 dent.

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

21 “(1) AUTHORIZED ACTIVITIES.—No informa-
22 tion provided to the Office in accordance with sub-
23 sections (d) or (h) may be disclosed to, retained by,
24 or used by any Federal department or agency, or
25 any component, officer, employee, or agent of the

1 Federal Government, except if the Director deter-
2 mines such disclosure, retention, or use is necessary
3 for—

4 “(A) a cybersecurity purpose;

5 “(B) the purpose of identifying—

6 “(i) a cybersecurity threat, including
7 the source of such threat; or

8 “(ii) a security vulnerability;

9 “(C) the purpose of responding to, or oth-
10 erwise preventing, or mitigating a specific
11 threat of—

12 “(i) death;

13 “(ii) serious bodily harm; or

14 “(iii) serious economic harm, includ-
15 ing a terrorist act or a use of a weapon of
16 mass destruction;

17 “(D) the purpose of responding to, inves-
18 tigating, prosecuting, or otherwise preventing or
19 mitigating a serious threat to a minor, includ-
20 ing sexual exploitation or threats to physical
21 safety; or

22 “(E) the purpose of preventing, inves-
23 tigating, disrupting, or prosecuting an offense
24 related to a threat—

1 “(i) described in subparagraphs (B)
2 through (D); or

3 “(ii) specified in section
4 105(d)(5)(A)(v) of the Cybersecurity Act
5 of 2015 (enacted as division N of the Con-
6 solidated Appropriations Act, 2016 (Public
7 Law 114–113; 6 U.S.C.
8 1504(d)(5)(A)(v))).

9 “(2) EXCEPTIONS.—

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

22 “(B) PRINCIPLES FOR SHARING SECURITY
23 VULNERABILITIES.—With respect to informa-
24 tion in a covered cybersecurity incident report
25 regarding a security vulnerability referred to in

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

7 “(3) PRIVACY AND CIVIL LIBERTIES.—Informa-
8 tion contained in reports submitted to the Office
9 pursuant to subsections (d) and (h) shall be re-
10 tained, used, and disseminated, where permissible
11 and appropriate, by the Federal Government in a
12 manner consistent with processes for the protection
13 of personal information adopted pursuant to section
14 105 of the Cybersecurity Act of 2015 (enacted as di-
15 vision N of the Consolidated Appropriations Act,
16 2016 (Public Law 114–113; 6 U.S.C. 1504)).

17 “(4) PROHIBITION ON USE OF INFORMATION IN
18 REGULATORY ACTIONS.—

19 “(A) IN GENERAL.—Information contained
20 in reports submitted to the Office pursuant to
21 subsections (d) and (h) may not be used by any
22 Federal, State, Tribal, or local government to
23 regulate, including through an enforcement ac-
24 tion, the lawful activities of any non-Federal en-
25 tity.

1 “(B) EXCEPTION.—A report submitted to
2 the Agency pursuant to subsection (d) or (h)
3 may, consistent with Federal or State regu-
4 latory authority specifically relating to the pre-
5 vention and mitigation of cybersecurity threats
6 to information systems, inform the development
7 or implementation of regulations relating to
8 such systems.

9 “(f) PROTECTIONS FOR REPORTING ENTITIES AND
10 INFORMATION.—Reports describing covered cybersecurity
11 incidents submitted to the Office by covered entities in ac-
12 cordance with subsection (d), as well as voluntarily-sub-
13 mitted cybersecurity incident reports submitted to the Of-
14 fice pursuant to subsection (h), shall be—

15 “(1) entitled to the protections against liability
16 described in section 106 of the Cybersecurity Act of
17 2015 (enacted as division N of the Consolidated Ap-
18 propriations Act, 2016 (Public Law 114–113; 6
19 U.S.C. 1505));

20 “(2) exempt from disclosure under section 552
21 of title 5, United States Code, as well as any provi-
22 sion of State, Tribal, or local freedom of information
23 law, open government law, open meetings law, open
24 records law, sunshine law, or similar law requiring
25 disclosure of information or records; and

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

4 “(g) NONCOMPLIANCE WITH REQUIRED REPORT-
5 ING.—

6 “(1) PURPOSE.—In the event a covered entity
7 experiences a cybersecurity incident but does not
8 comply with the reporting requirements under this
9 section, the Director may obtain information about
10 such incident by engaging directly such covered enti-
11 ty in accordance with paragraph (2) to request in-
12 formation about such incident, or, if the Director is
13 unable to obtain such information through such en-
14 gagement, by issuing a subpoena to such covered en-
15 tity, subject to paragraph (3), to gather information
16 sufficient to determine whether such incident is a
17 covered cybersecurity incident, and if so, whether ad-
18 ditional action is warranted pursuant to paragraph
19 (4).

20 “(2) INITIAL REQUEST FOR INFORMATION.—

21 “(A) IN GENERAL.—If the Director has
22 reason to believe, whether through public re-
23 porting, intelligence gathering, or other infor-
24 mation in the Federal Government’s possession,
25 that a covered entity has experienced a cyberse-

1 curity incident that may be a covered cyberse-
2 curity incident but did not submit pursuant to
3 subsection (d) to the Office a covered cyberse-
4 curity incident report relating thereto, the Di-
5 rector may request information from such cov-
6 ered entity to confirm whether the cybersecurity
7 incident at issue is a covered cybersecurity inci-
8 dent, and determine whether further examina-
9 tion into the details surrounding such incident
10 are warranted pursuant to paragraph (4).

11 “(B) TREATMENT.—Information provided
12 to the Office in response to a request under
13 subparagraph (A) shall be treated as if such in-
14 formation was submitted pursuant to the re-
15 porting procedures established in accordance
16 with subsection (d).

17 “(3) AUTHORITY TO ISSUE SUBPOENAS.—

18 “(A) IN GENERAL.—If, after the date that
19 is seven days from the date on which the Direc-
20 tor made a request for information in para-
21 graph (2), the Director has received no re-
22 sponse from the entity from which such infor-
23 mation was requested, or received an inad-
24 equate response, the Director may issue to such
25 entity a subpoena to compel disclosure of infor-

1 mation the Director considers necessary to de-
2 termine whether a covered cybersecurity inci-
3 dent has occurred and assess potential impacts
4 to national security, economic security, or pub-
5 lic health and safety, determine whether further
6 examination into the details surrounding such
7 incident are warranted pursuant to paragraph
8 (4), and if so, compel disclosure of such infor-
9 mation as is necessary to carry out activities
10 described in subsection (c).

11 “(B) CIVIL ACTION.—If a covered entity
12 does not comply with a subpoena, the Director
13 may bring a civil action in a district court of
14 the United States to enforce such subpoena. An
15 action under this paragraph may be brought in
16 the judicial district in which the entity against
17 which the action is brought resides, is found, or
18 does business. The court may punish a failure
19 to obey an order of the court to comply with the
20 subpoena as a contempt of court.

21 “(C) NON-APPLICABILITY OF PROTEC-
22 TIONS.—The protections described in subsection
23 (f) do not apply to a covered entity that is the
24 recipient of a subpoena under this paragraph
25 (3).

1 “(4) ADDITIONAL ACTIONS.—

2 “(A) EXAMINATION.—If, based on the in-
3 formation provided in response to a subpoena
4 issued pursuant to paragraph (3), the Director
5 determines that the cybersecurity incident at
6 issue is a significant cyber incident, or is part
7 of a group of related cybersecurity incidents
8 that together satisfy the definition of a signifi-
9 cant cyber incident, and a more thorough exam-
10 ination of the details surrounding such incident
11 is warranted in order to carry out activities de-
12 scribed in subsection (c), the Director may di-
13 rect the Office to conduct an examination of
14 such incident in order to enhance the Agency’s
15 situational awareness of cybersecurity threats
16 across critical infrastructure sectors, in a man-
17 ner consistent with privacy and civil liberties
18 protections under applicable law.

19 “(B) PROVISION OF CERTAIN INFORMA-
20 TION TO ATTORNEY GENERAL.—Notwith-
21 standing subsection (e)(4) and paragraph
22 (2)(B), if the Director determines, based on the
23 information provided in response to a subpoena
24 issued pursuant to paragraph (3) or identified
25 in the course of an examination under subpara-

1 graph (A), that the facts relating to the cyber-
2 security incident at issue may constitute
3 grounds for a regulatory enforcement action or
4 criminal prosecution, the Director may provide
5 such information to the Attorney General or the
6 appropriate regulator, who may use such infor-
7 mation for a regulatory enforcement action or
8 criminal prosecution.

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

21 “(i) NOTIFICATION TO IMPACTED COVERED ENTI-
22 TIES.—If the Director receives information regarding a
23 cybersecurity incident impacting a Federal agency relating
24 to unauthorized access to data provided to such Federal
25 agency by a covered entity, and with respect to which such

1 incident is likely to undermine the security of such covered
2 entity or cause operational or reputational damage to such
3 covered entity, the Director shall, to the extent prac-
4 ticable, notify such covered entity and provide to such cov-
5 ered entity such information regarding such incident as
6 is necessary to enable such covered entity to address any
7 such security risk or operational or reputational damage
8 arising from such incident.

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

12 “(k) SAVING PROVISION.—Nothing in this section
13 may be construed as modifying, superseding, or otherwise
14 affecting in any manner any regulatory authority held by
15 a Federal department or agency, including Sector Risk
16 Management Agencies, existing on the day before the date
17 of the enactment of this section, or any existing regulatory
18 requirements or obligations that apply to covered enti-
19 ties.”.

20 (b) REPORTS.—

21 (1) ON STAKEHOLDER ENGAGEMENT.—Not
22 later than 30 days before the date on which that the
23 Director of the Cybersecurity and Infrastructure Se-
24 curity Agency of the Department of Homeland Secu-
25 rity intends to issue an interim final rule under sub-

1 section (d)(1) of section 2220A of the Homeland Se-
2 curity Act of 2002 (as added by subsection (a)), the
3 Director shall submit to the Committee on Home-
4 land Security of the House of Representatives and
5 the Committee on Homeland Security and Govern-
6 mental Affairs of the Senate a report that describes
7 how the Director engaged stakeholders in the devel-
8 opment of such interim final rules.

9 (2) ON OPPORTUNITIES TO STRENGTHEN CY-
10 BERSECURITY RESEARCH.—Not later than one year
11 after the date of the enactment of this Act, the Di-
12 rector of the Cybersecurity and Infrastructure Secu-
13 rity Agency of the Department of Homeland Secu-
14 rity shall submit to the Committee on Homeland Se-
15 curity of the House of Representatives and the Com-
16 mittee on Homeland Security and Governmental Af-
17 fairs of the Senate a report describing how the
18 Cyber Incident Review Office of the Department of
19 Homeland Security (established pursuant to section
20 2220A of the Homeland Security Act of 2002, as
21 added by subsection (a)) has carried out activities
22 under subsection (c)(6) of such section 2220A by
23 proactively identifying opportunities to use cyberse-
24 curity incident data to inform and enable cybersecu-

1 rity research carried out by academic institutions
2 and other private sector organizations.

3 (c) TITLE XXII TECHNICAL AND CLERICAL AMEND-
4 MENTS.—

5 (1) TECHNICAL AMENDMENTS.—

6 (A) HOMELAND SECURITY ACT OF 2002.—

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

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

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

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

19 (III) by redesignating the second
20 paragraph (12) (relating to the .gov
21 internet domain) as paragraph (13);
22 and

23 (IV) by redesignating the third
24 paragraph (12) (relating to carrying

1 out such other duties and responsibil-
2 ities) as paragraph (14);

3 (ii) in the first section 2215 (6 U.S.C.
4 665; relating to the duties and authorities
5 relating to .gov internet domain), by
6 amending the section enumerator and
7 heading to read as follows:

8 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**
9 **INTERNET DOMAIN.”;**

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

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

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

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

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

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

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

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

7 (vii) in section 2217 (6 U.S.C. 665f;
8 relating to Cybersecurity Education and
9 Training Programs), by amending the sec-
10 tion enumerator and heading to read as
11 follows:

12 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**
13 **PROGRAMS.”.**

14 (B) CONSOLIDATED APPROPRIATIONS ACT,
15 2021.—Paragraph (1) of section 904(b) of divi-
16 sion U of the Consolidated Appropriations Act,
17 2021 (Public Law 116–260) is amended, in the
18 matter preceding subparagraph (A), by insert-
19 ing “of 2002” after “Homeland Security Act”.

20 (2) CLERICAL AMENDMENT.—The table of con-
21 tents in section 1(b) of the Homeland Security Act
22 of 2002 is amended by striking the items relating to
23 sections 2214 through 2217 and inserting the fol-
24 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.”.

