# 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:

**SEC. 15___. CYBER INCIDENT REVIEW OFFICE.**

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

**"SEC. 2220A. CYBER INCIDENT REVIEW OFFICE.**

''(a) DEFINITIONS.—In this section:

''(1) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(2) COVERED ENTITY.—The term 'covered entity' means an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the reporting requirements and procedures issued pursuant to subsection (d).

''(3) COVERED CYBSECURITY INCIDENT.—The term 'covered cybersecurity incident' means a cybersecurity incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the reporting requirements and procedures issued pursuant to subsection (d).

''(4) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(5) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114-113; 6 U.S.C. 1501).

''(6) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(7) DEFENSIVE MEASURE.—The term 'defensive measure' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(8) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' has the meaning given such term in section 2222(5).

''(9) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9)).

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

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

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

''(12) SECURITY CONTROL.—The term 'security control' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(13) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(14) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident, or a group of related cyber incidents, that the Director determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

''(15) SUPPLY CHAIN ATTACK.—The term 'supply chain attack' means an attack that allows an adversary to utilize implants or other vulnerabilities in-

serted into information technology hardware, software, operating systems, peripherals (such as information technology products), or services at any point during the life cycle in order to infiltrate the networks of third parties where such products, services, or technologies are deployed.

''(b) CYBER INCIDENT REVIEW OFFICE.—There is established in the Agency a Cyber Incident Review Office (in this section referred to as the 'Office') to receive, aggregate, and analyze reports related to covered cybersecurity incidents submitted by covered entities in furtherance of the activities specified in subsection (c) of this section and sections 2202(e), 2209(c), and 2203 to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.

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

''(1) receive, aggregate, analyze, and secure reports from covered entities related to a covered cybersecurity incident to assess the effectiveness of security controls and identify tactics, techniques, and procedures adversaries use to overcome such controls;

''(2) facilitate the timely sharing between relevant critical infrastructure owners and operators and, as appropriate, the intelligence community of information relating to covered cybersecurity incidents, particularly with respect to an ongoing cybersecurity threat or security vulnerability;

''(3) for a covered cybersecurity incident that also satisfies the definition of a significant cyber incident, or are part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding such covered cybersecurity incident or group of such incidents and identify ways to prevent or mitigate similar incidents in the future;

''(4) with respect to covered cybersecurity incident reports under subsection (d) involving an ongoing cybersecurity threat or security vulnerability, immediately review such reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other Divisions within the Agency, as appropriate;

''(5) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on cov-

ered cybersecurity incident reports under subsection (d);

''(6) leverage information gathered regarding cybersecurity incidents to enhance the quality and effectiveness of bi-directional information sharing and coordination efforts with appropriate stakeholders, including sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, including by establishing mechanisms to receive feedback from such stakeholders regarding how the Agency can most effectively support private sector cybersecurity; and

''(6) proactively identify opportunities, in accordance with the protections specified in subsections (e) and (f), to leverage and utilize data on cybersecurity incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable.

''(d) COVERED CYBERSECURITY INCIDENT REPORTING REQUIREMENTS AND PROCEDURES.—

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

ment Agencies and the heads of other Federal departments and agencies, as appropriate, shall, after a 60 day consultative period, followed by a 90 day comment period with appropriate stakeholders, including sector coordinating councils, publish in the Federal Register an interim final rule implementing this section. Notwithstanding section 553 of title 5, United States Code, such rule shall be effective, on an interim basis, immediately upon publication, but may be subject to change and revision after public notice and opportunity for comment. The Director shall issue a final rule not later than one year after publication of such interim final rule. Such interim final rule shall—

''(A) require covered entities to submit to the Office reports containing information relating to covered cybersecurity incidents; and

''(B) establish procedures that clearly describe—

''(i) the types of critical infrastructure entities determined to be covered entities;

''(ii) the types of cybersecurity incidents determined to be covered cybersecurity incidents;

''(iii) the mechanisms by which covered cybersecurity incident reports under subparagraph (A) are to be submitted, including—

''(I) the contents, described in paragraph (4), to be included in each such report, including any supplemental reporting requirements;

''(II) the timing relating to when each such report should be submitted; and

''(III) the format of each such report;

''(iv) describe the manner in which the Office will carry out enforcement actions under subsection (g), including with respect to the issuance of subpoenas, conducting examinations, and other aspects relating to noncompliance; and

''(v) any other responsibilities to be carried out by covered entities, or other procedures necessary to implement this section.

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

ered entities for purposes of this section, the Secretary, acting through the Director, in consultation with Sector Risk Management Agencies and the heads of other Federal departments and agencies, as appropriate, shall consider—

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

''(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country;

''(C) the extent to which damage, disruption, or unauthorized access to such and entity will disrupt the reliable operation of other critical infrastructure assets; and

''(D) the extent to which an entity or sector is subject to existing regulatory requirements to report cybersecurity incidents, and the possibility of coordination and sharing of reports between the Office and the regulatory authority to which such entity submits such other reports.

''(3) OUTREACH TO COVERED ENTITIES.—

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

''(B) ELEMENTS.—The outreach and education campaign under subparagraph (A) shall include the following:

''(i) Overview of the interim final rule and final rule issued pursuant to this section.

''(ii) Overview of reporting requirements and procedures issued pursuant to paragraph (1).

''(iii) Overview of mechanisms to submit to the Office covered cybersecurity incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

''(iv) Overview of the protections afforded to covered entities for complying with requirements under subsection (f).

''(v) Overview of the steps taken under subsection (g) when a covered entity is not in compliance with the reporting requirements under paragraph (1).

''(C) COORDINATION.—The Director may conduct the outreach and education campaign under subparagraph (A) through coordination with the following:

''(i) The Critical Infrastructure Partnership Advisory Council established pursuant to section 871.

''(ii) Information Sharing and Analysis Organizations.

''(iii) Any other means the Director determines to be effective to conduct such campaign.

''(4) COVERED CYBERSECURITY INCIDENTS.—

''(A) CONSIDERATIONS.—In accordance with subparagraph (B), in determining which types of incidents are covered cybersecurity incidents for purposes of this section, the Director shall consider—

''(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

''(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

''(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

''(B) MINIMUM THRESHOLDS.—For a cybersecurity incident to be considered a covered cybersecurity incident a cybersecurity incident shall, at a minimum, include at least one of the following:

''(i) Unauthorized access to an information system or network that leads to loss of confidentiality, integrity, or availability of such information system or network, or has a serious impact on the safety and resiliency of operational systems and processes.

''(ii) Disruption of business or industrial operations due to a denial of service attack, a ransomware attack, or exploitation of a zero-day vulnerability, against—

''(I) an information system or network; or

''(II) an operational technology system or process.

''(iii) Unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by a compromise of, a cloud service provider, managed service provider, other third-party data hosting provider, or supply chain attack.

''(5) REPORTS.—

''(A) TIMING.—

''(i) IN GENERAL.—The Director, in consultation with Sector Risk Management Agencies and the heads of other Federal departments and agencies, as appropriate, shall establish reporting timelines for covered entities to submit promptly to the Office covered cybersecurity incident reports, as the Director determines reasonable and appropriate based on relevant factors, such as the nature, severity, and complexity of the covered cybersecurity incident at issue and the time required for investigation, but in no case may the Director require reporting by a covered entity earlier than 72

hours after confirmation that a covered cybersecurity incident has occurred.

''(ii) CONSIDERATIONS.—In determining reporting timelines under clause (i), the Director shall—

''(I) consider any existing regulatory reporting requirements, similar in scope purpose, and timing to the reporting requirements under this section, to which a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

''(II) balance the Agency's need for situational awareness with a covered entity's ability to conduct incident response and investigations.

''(B) THIRD PARTY REPORTING.—

''(i) IN GENERAL.—A covered entity may submit a covered cybersecurity incident report through a third party entity or Information Sharing and Analysis Organization.

"(ii) DUTY TO ENSURE COMPLIANCE.—Third party reporting under this subparagraph does not relieve a covered entity of the duty to ensure compliance with the requirements of this paragraph.

"(C) SUPPLEMENTAL REPORTING.—A covered entity shall submit promptly to the Office, until such date that such covered entity notifies the Office that the cybersecurity incident investigation at issue has concluded and the associated covered cybersecurity incident has been fully mitigated and resolved, periodic updates or supplements to a previously submitted covered cybersecurity incident report if new or different information becomes available that would otherwise have been required to have been included in such previously submitted report. In determining reporting timelines, the Director may choose to establish a flexible, phased reporting timeline for covered entities to report information in a manner that aligns with investigative timelines and allows covered entities to prioritize incident response efforts over compliance.

"(D) CONTENTS.—Covered cybersecurity incident reports submitted pursuant to this section shall contain such information as the Director prescribes, including the following information, to the extent applicable and available, with respect to a covered cybersecurity incident:

"(i) A description of the covered cybersecurity incident, including identification of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident, and the estimated date range of such incident.

"(ii) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures relevant to such incident.

"(iii) Where applicable, any identifying information related to the actor reasonably believed to be responsible for such incident.

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

been, accessed or acquired by an unauthorized person.

''(v) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the covered entity or, where applicable, an authorized agent of such covered entity, or, where applicable, the service provider, acting with the express permission, and at the direction, of such covered entity, to assist with compliance with the requirements of this section.

''(6) RESPONSIBILITIES OF COVERED ENTITIES.—Covered entities that experience a covered cybersecurity incident shall coordinate with the Office to the extent necessary to comply with this section, and, to the extent practicable, cooperate with the Office in a manner that supports enhancing the Agency's situational awareness of cybersecurity threats across critical infrastructure sectors.

''(7) HARMONIZING REPORTING REQUIREMENTS.—In establishing the reporting requirements and procedures under paragraph (1), the Director shall, to the maximum extent practicable—

''(A) review existing regulatory requirements, including the information required in such reports, to report cybersecurity incidents that may apply to covered entities, and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

''(B) coordinate with other regulatory authorities that receive reports relating to cybersecurity incidents to identify opportunities to streamline reporting processes, and where feasible, enter into agreements with such authorities to permit the sharing of such reports with the Office, consistent with applicable law and policy, without impacting the Office's ability to gain timely situational awareness of a covered cybersecurity incident or significant cyber incident.

''(e) DISCLOSURE, RETENTION, AND USE OF INCIDENT REPORTS.—

''(1) AUTHORIZED ACTIVITIES.—No information provided to the Office in accordance with subsections (d) or (h) may be disclosed to, retained by, or used by any Federal department or agency, or any component, officer, employee, or agent of the

Federal Government, except if the Director determines such disclosure, retention, or use is necessary for—

''(A) a cybersecurity purpose;

''(B) the purpose of identifying—

''(i) a cybersecurity threat, including the source of such threat; or

''(ii) a security vulnerability;

''(C) the purpose of responding to, or otherwise preventing, or mitigating a specific threat of—

''(i) death;

''(ii) serious bodily harm; or

''(iii) serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

''(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation or threats to physical safety; or

''(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense related to a threat—

"(i) described in subparagraphs (B) through (D); or

"(ii) specified in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1504(d)(5)(A)(v))).

"(2) EXCEPTIONS.—

"(A) RAPID, CONFIDENTIAL, BI-DIRECTIONAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cybersecurity incident report submitted pursuant to this section, the Office shall immediately review such report to determine whether the incident that is the subject of such report is connected to an ongoing cybersecurity threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

"(B) PRINCIPLES FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cybersecurity incident report regarding a security vulnerability referred to in

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

''(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in reports submitted to the Office pursuant to subsections (d) and (h) shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in a manner consistent with processes for the protection of personal information adopted pursuant to section 105 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1504)).

''(4) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—

''(A) IN GENERAL.—Information contained in reports submitted to the Office pursuant to subsections (d) and (h) may not be used by any Federal, State, Tribal, or local government to regulate, including through an enforcement action, the lawful activities of any non-Federal entity.

''(B) EXCEPTION.—A report submitted to the Agency pursuant to subsection (d) or (h) may, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems.

''(f) PROTECTIONS FOR REPORTING ENTITIES AND INFORMATION.—Reports describing covered cybersecurity incidents submitted to the Office by covered entities in accordance with subsection (d), as well as voluntarily-submitted cybersecurity incident reports submitted to the Office pursuant to subsection (h), shall be—

''(1) entitled to the protections against liability described in section 106 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1505));

''(2) exempt from disclosure under section 552 of title 5, United States Code, as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records; and

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

''(g) NONCOMPLIANCE WITH REQUIRED REPORTING.—

''(1) PURPOSE.—In the event a covered entity experiences a cybersecurity incident but does not comply with the reporting requirements under this section, the Director may obtain information about such incident by engaging directly such covered entity in accordance with paragraph (2) to request information about such incident, or, if the Director is unable to obtain such information through such engagement, by issuing a subpoena to such covered entity, subject to paragraph (3), to gather information sufficient to determine whether such incident is a covered cybersecurity incident, and if so, whether additional action is warranted pursuant to paragraph (4).

''(2) INITIAL REQUEST FOR INFORMATION.—

''(A) IN GENERAL.—If the Director has reason to believe, whether through public reporting, intelligence gathering, or other information in the Federal Government's possession, that a covered entity has experienced a cyberse-

curity incident that may be a covered cybersecurity incident but did not submit pursuant to subsection (d) to the Office a covered cybersecurity incident report relating thereto, the Director may request information from such covered entity to confirm whether the cybersecurity incident at issue is a covered cybersecurity incident, and determine whether further examination into the details surrounding such incident are warranted pursuant to paragraph (4).

''(B) TREATMENT.—Information provided to the Office in response to a request under subparagraph (A) shall be treated as if such information was submitted pursuant to the reporting procedures established in accordance with subsection (d).

''(3) AUTHORITY TO ISSUE SUBPOENAS.—

''(A) IN GENERAL.—If, after the date that is seven days from the date on which the Director made a request for information in paragraph (2), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of infor-

mation the Director considers necessary to determine whether a covered cybersecurity incident has occurred and assess potential impacts to national security, economic security, or public health and safety, determine whether further examination into the details surrounding such incident are warranted pursuant to paragraph (4), and if so, compel disclosure of such information as is necessary to carry out activities described in subsection (c).

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

''(C) NON-APPLICABILITY OF PROTECTIONS.—The protections described in subsection (f) do not apply to a covered entity that is the recipient of a subpoena under this paragraph (3).

''(4) ADDITIONAL ACTIONS.—

''(A) EXAMINATION.—If, based on the information provided in response to a subpoena issued pursuant to paragraph (3), the Director determines that the cybersecurity incident at issue is a significant cyber incident, or is part of a group of related cybersecurity incidents that together satisfy the definition of a significant cyber incident, and a more thorough examination of the details surrounding such incident is warranted in order to carry out activities described in subsection (c), the Director may direct the Office to conduct an examination of such incident in order to enhance the Agency's situational awareness of cybersecurity threats across critical infrastructure sectors, in a manner consistent with privacy and civil liberties protections under applicable law.

''(B) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—Notwithstanding subsection (e)(4) and paragraph (2)(B), if the Director determines, based on the information provided in response to a subpoena issued pursuant to paragraph (3) or identified in the course of an examination under subpara-

graph (A), that the facts relating to the cybersecurity incident at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such information to the Attorney General or the appropriate regulator, who may use such information for a regulatory enforcement action or criminal prosecution.

''(h) VOLUNTARY REPORTING OF CYBER INCIDENTS.—The Agency shall receive cybersecurity incident reports submitted voluntarily by entities that are not covered entities, or concerning cybersecurity incidents that do not satisfy the definition of covered cybersecurity incidents but may nevertheless enhance the Agency's situational awareness of cybersecurity threats across critical infrastructure sectors. The protections under this section applicable to covered cybersecurity incident reports shall apply in the same manner and to the same extent to voluntarily-submitted cybersecurity incident reports under this subsection.

''(i) NOTIFICATION TO IMPACTED COVERED ENTITIES.—If the Director receives information regarding a cybersecurity incident impacting a Federal agency relating to unauthorized access to data provided to such Federal agency by a covered entity, and with respect to which such

incident is likely to undermine the security of such covered entity or cause operational or reputational damage to such covered entity, the Director shall, to the extent practicable, notify such covered entity and provide to such covered entity such information regarding such incident as is necessary to enable such covered entity to address any such security risk or operational or reputational damage arising from such incident.

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

(b) REPORTS.—

(1) ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days before the date on which that the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security intends to issue an interim final rule under subsection (d)(1) of section 2220A of the Homeland Security Act of 2002 (as added by subsection (a)), the Director shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that describes how the Director engaged stakeholders in the development of such interim final rules.

(2) ON OPPORTUNITIES TO STRENGTHEN CYBERSECURITY RESEARCH.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report describing how the Cyber Incident Review Office of the Department of Homeland Security (established pursuant to section 2220A of the Homeland Security Act of 2002, as added by subsection (a)) has carried out activities under subsection (c)(6) of such section 2220A by proactively identifying opportunities to use cybersecurity incident data to inform and enable cybersecurity research carried out by academic institutions and other private sector organizations.

(c) TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.—

(1) TECHNICAL AMENDMENTS.—

(A) HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(i) in section 2202 (6 U.S.C. 652)—

(I) in paragraph (11), by striking ''and'' after the semicolon;

(II) in the first paragraph (12) (relating to appointment of a Cybersecurity State Coordinator) by striking ''as described in section 2215; and'' and inserting ''as described in section 2217;'';

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

(IV) by redesignating the third paragraph (12) (relating to carrying out such other duties and responsibilities) as paragraph (14);

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

**"SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.";**

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

**"SEC. 2216. JOINT CYBER PLANNING OFFICE.";**

(iv) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

**"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";**

(v) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

**"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";**

(vi) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

**"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and**

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

Training Programs), by amending the section enumerator and heading to read as follows:

**"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".**

(B) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following 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.''.