Calendar No. 632

117TH CONGRESS *2d Session*	SENATE	REPORT 117–248

CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2540

TO MAKE TECHNICAL CORRECTIONS TO TITLE XXII OF THE HOMELAND SECURITY ACT OF 2002, AND FOR OTHER PURPOSES

DECEMBER 13, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 632

117TH CONGRESS *2d Session* | SENATE | REPORT 117–248

CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

DECEMBER 13, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2540]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2540) to make technical corrections to title XXII of the Homeland Security Act of 2002, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	2
IV. Section-by-Section Analysis of the Bill, as Reported	2
V. Evaluation of Regulatory Impact	3
VI. Congressional Budget Office Cost Estimate	4
VII. Changes in Existing Law Made by the Bill, as Reported	4

I. PURPOSE AND SUMMARY

S. 2540, the *CISA Technical Corrections and Improvements Act of 2021*, makes technical and conforming edits to Title XXII of the Homeland Security Act of 2002. Following the adoption of the Cybersecurity and Infrastructure Security Agency Act of 2018, which established the Cybersecurity and Infrastructure Security Agency (CISA) and created Title XXII of the Homeland Security Act of 2002, Congress has amended the statute several times, which has

caused several drafting errors to occur in the statute. S. 2540 would correct those drafting errors.

II. Background and Need for the Legislation

On November 16, 2018, the Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law.[1] The Act created CISA and Title XXII of the Homeland Security Act of 2002. Congress has amended the title several times since. Some of those amendments and other provisions of law have been enacted close in time to one another, resulting in drafting errors in the statute, such as multiple section 2215s. S. 2540 would correct those drafting errors identified by the U.S. Senate Office of Legislative Counsel, as well as consolidate definitions cross-referenced from other parts of Title XXII, and other laws, at the beginning of the title.

III. Legislative History

Senator Portman (R–OH) introduced S. 2540, the *CISA Technical Corrections and Improvements Act of 2021*, on July 29, 2021, along with Senator Peters (D–MI). The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. Senator Hassan (D–NH) joined as a cosponsor on November 2, 2021. The Committee considered S. 2540 at a business meeting on November 3, 2021. During the business meeting, Senators Portman and Peters offered a substitute amendment, which was adopted by voice vote *en bloc* with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present. The Committee ordered the bill, as amended, reported favorably by voice vote *en bloc* with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section designates the name of the bill as the "CISA Technical Corrections and Improvements Act of 2021."

Section 2. Redesignations

Subsection (a) amends Subtitle A of title XXII of the Homeland Security Act of 2002 by redesignating several sections.[2]

Subsection (b) makes technical and conforming amendments to Section 2202(c) of the Homeland Security Act of 2002.

Subsection (c) makes an additional technical amendment to section 904(b)(1) of the DOTGOV Act of 2020 and provides that the amendment made shall take effect as if enacted as part of the DOTGOV Act of 2020.

---

[1] Pub. L. 115–278.

[2] The technical corrections set forth in section 9 of the bill were incorporated in the National Defense Authorization Act for Fiscal Year 2022 (Pub. L. 117–81, Sec. 1547(b)(1)), which became law before this bill was reported out of committee. These amendments are now moot and are not reflected in Section VII of this report.

Section 3. Consolidation of definitions

Subsection (a) amends title XXII of the Homeland Security Act of 2002 by inserting a new Section 2200 before the subtitle A heading.

Section 2200 defines in the Homeland Security Act of 2002 the terms "agency," "agency information," appropriate congressional committees," "critical infrastructure information," "cyber threat indicator," "cybersecurity purpose," "cybersecurity risk," "cybersecurity threat," "defensive measure," "Homeland Security Enterprise," "Incident," "Information Sharing and Analysis Organization," "information system," "intelligence community," "monitor," "national cybersecurity asset response activities," "national security system," "Sector Risk Management Agency," "security control," "security vulnerability," and "sharing."

Subsection (b) makes technical and conforming amendments to the Homeland Security Act of 2002.

Subsection (c) amends the table of contents in section 1(b) of the Homeland Security Act of 2002.

Subsection (d) amends the definitions in section 102 of the Cybersecurity Act of 2015.

Section 4. Additional technical and conforming amendments

Subsection (a) makes technical and conforming amendments to the Federal Cybersecurity Enhancement Act of 2015.

Subsection (b) makes technical and conforming amendments to section 2811(b)(4)(D) of the Public Health Service Act.

Subsection (c) makes technical and conforming amendments to section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act of Fiscal Year 2021.

Subsection (d) makes technical and conforming amendments to section 113B of the National Security Act of 1947.

Subsection (e) makes technical and conforming amendments to section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020.

Subsection (f) makes technical and conforming amendments to section 21(a)(8)(B) of the Small Business Act.

Subsection (g) makes technical and conforming amendments to section 70101(2) of title 46 of the United States Code.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, December 16, 2021.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2540, the CISA Technical Corrections and Improvements Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 2540, CISA Technical Corrections and Improvements Act of 2021
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on November 3, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	0	not estimated

		Mandate Effects	
Statutory pay-as-you-go procedures apply?	No		
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 2540 would make technical changes to, but not substantively alter, provisions of title 6, U.S. Code, which govern the authority of the Cybersecurity and Infrastructure Security Agency (CISA).

S. 2540 would not impose any new requirements or duties on CISA. As a result, CBO estimates that enacting the bill would have no effect on the federal budget.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

CONSOLIDATED APPROPRIATIONS ACT OF 2021

* * * * * * *

TITLE IX—DOTGOV ACT OF 2020

* * * * * * *

SEC. 901. SHORT TITLE

* * * * * * *

SEC. 904. DUTIES OF DEPARTMENT OF HOMELAND SECURITY.

(a) * * *

(b) DUTIES AND AUTHORITIES RELATING TO THE .GOV INTERNET DOMAIN.—

(1) IN GENERAL.—Subtitle A of title XXII of the ⟦Homeland Security Act⟧ *Homeland Security Act of 2002* (6 U.S.C. 651 et seq.) is amended—

* * * * * * *

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Sec.2200. Definitions.

SUBTITLE A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

Sec. 2201. Definitions.
Sec. 2202. Cybersecurity and Infrastructure Security Agency.
Sec. 2203. Cybersecurity Division.
Sec. 2204. Infrastructure Security Division.
Sec. 2205. Enhancement of Federal and non-Federal cybersecurity.
Sec. 2206. Net guard.
Sec. 2207. Cyber Security Enhancement Act of 2002.
Sec. 2208. Cybersecurity recruitment and retention.
Sec. 2209. National cybersecurity and communications integration center.
Sec. 2210. Cybersecurity plans.
Sec. 2211. Cybersecurity strategy.
Sec. 2212. Clearances.
Sec. 2213. Federal intrusion detection and prevention system.
⟦Sec. 2214. National Asset Database.⟧
⟦Sec. 2215. Duties and authorities relating to .gov internet domain.⟧
⟦Sec. 2215. Joint cyber planning office.⟧
⟦Sec. 2215. Cybersecurity State Coordinator.⟧
⟦Sec. 2215. Sector Risk Management Agencies.⟧
⟦Sec. 2216. Cybersecurity Advisory Committee.⟧
⟦Sec. 2217. Cybersecurity education and training programs.⟧
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.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SEC. 2200. DEFINITIONS

Except as otherwise specifically provided, in this title:

(1) AGENCY.—The term "Agency" means the Cybersecurity and Infrastructure Security Agency.

(2) AGENCY INFORMATION.—The term "agency information" means information collected or maintained by or on behalf of an agency.

(3) AGENCY INFORMATION SYSTEM.—The term "agency information system" means an information system used or operated by an agency or by another entity on behalf of an agency.

(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committee" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives

(5) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violated Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(6) CYBER THREAT INDICATOR.—The term "cyber threat indicator" means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for

the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the infomation exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(7) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(8) CYBERSECURITY RISK.—The term "cybersecurity risk"—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(9) CYBERSECURITY THREAT

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(10) DEFENSE MEASURE

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(11) HOMELAND SECURITY ENTERPRISE.—The term "Homeland Security Enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

(12) INCIDENT.—The term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

(13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(14) INFORMATION SYSTEM.—The term "information system" has the meaning given the term in section 3502 of title 44, United States Code

(15) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 2 1947 (50 U.S.C. 3003(4)).

(16) MONITOR.—The term "monitor" means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(17) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term "national cybersecurity asset response activities" means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(18) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given the term in section 11103 of title 40, United States Code.

(19) SECTOR RISK MANAGEMENT AGENCY.—The term "Sector Risk Management Agency" means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

(20) SECURITY CONTROL.—The term "security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(21) SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(22) SHARING.—The term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

SUBTITLE A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

[SEC. 2201. DEFINITIONS.

[In this subtitle:

[(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" has the meaning given the term in section 2222.

[(2) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given the term in section 2209.

[(3) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given the term in section 102(5) of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

[(4) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term "national cybersecurity asset response activities"' means—

[(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

[(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

[(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

[(D) facilitating information sharing and operational coordination with threat response; and

[(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

[(5) SECTOR RISK MANAGEMENT AGENCY.—The term "Sector Risk Management Agency" means a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

[(6) SHARING.—The term "sharing" has the meaning given the term in section 2209.

[(7) SLTT ENTITY.—The term "SLTT entity" means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof.]

SEC. 2201. DEFINITION

In this subtitle, *the term "Cybersecurity Advisory Committee" means the advisory committee established under section 2219(a).*

* * * * * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) REDESIGNATION.—

(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the "Cybersecurity and Infrastructure Security Agency" [(in this subtitle referred to as the "Agency")].

* * * * * * *

(b) * * *

(c) RESPONSIBILITIES.—The Director shall—

(1) * * *

* * * * * * *

(11) provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security; [and]

(12) appoint a Cybersecurity State Coordinator in each State, as described in [section 2215] *section 2217*; [and]

[(12)] *(13)* carry out the duties and authorities relating to the .gov internet domain, as described in section 2215; and

[(12)] *(14)* carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) * * *

(e) * * *

(f) COMPOSITION.—The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an *Executive* Assistant Director.

(2) The Infrastructure Security Division, headed by an *Executive* Assistant Director.

* * * * * * *

SEC. 2203. CYBERSECURITY DIVISION

(a) ESTABLISHMENT.—

(1) * * *

(2) EXECUTIVE ASSISTANT DIRECTOR.—The Cybersecurity Division shall be headed by an Executive Assistant Director for Cybersecurity (in this section referred to [as the "Assistant Director"] *as the "Executive Assistant Director"*), who shall—

* * * * * * *

SEC. 2204. INFRASTRUCTURE SECURITY DIVISION

(a) ESTABLISHMENT.—

(1) * * *

(2) EXECUTIVE ASSISTANT DIRECTOR.—The Infrastructure Security Division shall be headed by an Executive Assistant Director for Infrastructure Security (in this section referred to [as the "Assistant Director"] *as the Executive Assistant Director*), who shall—

* * * * * * *

SEC. 2209. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

[(a) DEFINITIONS.—In this section—

[(1) the term "cybersecurity purpose" has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

[(2) the term "cybersecurity risk"—

[(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

[(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

[(3) the terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in section 102 of the Cybersecurity Act of 2015;

[(4) the term "cybersecurity vulnerability" has the meaning given the term "security vulnerability" in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

[(5) the term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;

[(6) the term "information sharing and analysis organization" has the meaning given that term in section 2222(5);

[(7) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code;

[(8) the term "security vulnerability" has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and

[(9) the term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).]

[(b)] *(a)* * * *

[(c)] *(b)* * * *

[(d)] *(c)* COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community[, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))];

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) [information sharing and analysis organizations] *Information Sharing and Analysis Organizations*, including information sharing and analysis centers;

[(e)] *(d)* PRINCIPLES.—In carrying out the functions under [subsection (c)] *subsection (b)*, the Center shall ensure—

(1) to the extent practicable, that—

(A) * * *

* * * * * * *

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) [information sharing and analysis organizations] *Information Sharing and Analysis Organizations*; and

(III) other appropriate non-Federal partners;

(F) * * *

* * * * * * *

[(f)] *(e)* * * *

[(g)] *(f)* * * *

[(h)] *(g)* * * *
[(i)] *(h)* * * *
[(j)] *(i)* * * *
[(k)] *(j)* REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of enactment of this subsection, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with [subsection (c)(8)] *subsection (b)(8)*.
[(l)] *(k)* * * *
[(m)] *(l)* * * *
[(n)] *(m)* * * *
[(o)] *(n)* * * *
(1) * * *
(2) AUTHORITY.—
(A) IN GENERAL.—If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe such security vulnerability relates to critical infrastructure and affects a covered device or system, and the Director is unable to identify the entity at risk that owns or operates such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk, in order to carry out a function authorized under [subsection (c)(12)] *subsection (b)(12)*.
(B) * * *
(C) * * *
(3) COORDINATION.—
(A) * * *
(B) * * *
(i) issued to carry out a function described in [subsection (c)(12)] *subsection (b)(12)*; and
(ii) * * *

SEC. 2210. CYBERSECURITY PLANS.

[(a) DEFINITIONS.—In this section—
(1) the term "agency information system" means an information system used or operated by an agency or by another entity on behalf of an agency;
(2) the terms "cybersecurity risk" and "information system" have the meanings given those terms in section 2209;
(3) 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)); and
(4) the term "national security system" has the meaning given the term in section 11103 of title 40, United States Code.]
[(b)] *(a)* * * *
[(c)] *(b)* CYBER INCIDENT RESPONSE PLAN.—The Director of Cybersecurity and Infrastructure Security shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, [information sharing and analysis organizations (as defined in section 2222(5))] *Information*

Sharing and Analysis Organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, update not less often than biennially, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks [(as defined in section 2209)] to critical infrastructure. The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate such stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response.

[(d)] *(c)* NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under [subsection (c)] *subsection (b)*, shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

SEC. 2211. CYBERSECURITY STRATEGY.

(a) * * *

* * * * * * *

(g) * * *

[(h) DEFINITION.—In this section, the term "Homeland Security Enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.]

SEC. 2212. CLEARANCES.

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector [information sharing and analysis organizations (as defined in section 2222(5))] *Information Sharing and Analysis Organization*, owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

SEC. 2213. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

[(a) DEFINITIONS.—In this section—

[(1) the term "agency" has the meaning given the term in section 3502 of title 44, United States Code;

[(2) the term "agency information" means information collected or maintained by or on behalf of an agency;

[(3) the term "agency information system" has the meaning given the term in section 2210; and

[(4) the terms "cybersecurity risk" and "information system" have the meanings given those terms in section 2209.]

[(b)] *(a)* * * *

[(c)] *(b)* ACTIVITIES.—In carrying out [subsection (b)] *subsection a*, the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of

the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with ⟦subsection (b)⟧ *subsection (a)*;

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

⟦(d)⟧ *(c)* PRINCIPLES.—In carrying out ⟦subsection (b)⟧ *subsection a*, the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

⟦(e)⟧ *(d)* PRIVATE ENTITIES.—

(1) CONDITIONS.—A private entity described in ⟦subsection (c)(2)⟧ *subsection(b)(2)* may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under ⟦subsection (c)(1)⟧ *subsection (b)(1)*, including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to ⟦subsection (c)(2)⟧ *subsection(b)(2)* or as part of another contract with the Secretary.

(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to ⟦subsection (c)(2)⟧ *subsection(b)(2)*.

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

⟦(f)⟧ *(e)* PRIVACY OFFICER REVIEW.—Not later than 1 year after the date of enactment of this section, the Privacy Officer appointed under section 222, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

* * * * * * *

SEC. ⟦2215⟧ *2216.* JOINT CYBER PLANNING OFFICE

(a) * * *

* * * * * * *

(d) CONSULTATION.—In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

(1) State, local, federally-recognized Tribal, and territorial governments;

(2) ⟦information sharing and analysis organizations⟧ *Information Sharing and Analysis Organizations*, including information sharing and analysis centers;

(3) owners and operators of critical information systems

(4) private entities; and

(5) other appropriate representatives or entities, as determined by the Secretary.

(e) * * *

⟦(f) DEFINITIONS.—In this section:

⟦(1) CYBER DEFENSE OPERATION.—The term "cyber defense" operation means defensive activities performed for a cybersecurity purpose.

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

⟦(3) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given such terms in section 2209.

[(4) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "information sharing and analysis organization" has the meaning given such term in section 2222(5).]

(f) CYBER DEFENSE OPERATION DEFINED.—*In this section, the term "cyber defense operation" means the use of a defensive measure.*

* * * * * * *

SEC. [2215] *2217*. CYBERSECURITY STATE COORDINATOR.

* * * * * * *

SEC. [2215] *2218*. SECTOR RISK MANAGEMENT AGENCIES.

(a) * * *
(b) * * *
(c) * * *
(1) * * *
(2) * * *
(3) * * *
(4) * * *

(A) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through [information sharing and analysis organizations] *Information Sharing and Analysis Organizations* and the national cybersecurity and communications integration center established pursuant to section 2209;

* * * * * * *

SEC. [2216] *2219*. CYBERSECURITY ADVISORY COMMITTEE.

* * * * * * *

SEC. [2217] *2220*. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.

* * * * * * *

Subtitle B—Critical Infrastructure Information

* * * * * * *

SEC. 2222. DEFINITIONS

In this subtitle:

(1) * * *
(2) * * *

[(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

[(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates

Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

[(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

[(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.]

[(4)] *(3)* CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term "critical infrastructure protection program" means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

[(5) INFORMATION SHARING AND ANALYSIS.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

[(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

[(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

[(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).]

[(6)] *(4)* PROTECTED SYSTEM.—The term "protected system"—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

[(7)] *(5)* VOLUNTARY.—

(A) IN GENERAL.—The term "voluntary", in the case of any submittal of critical infrastructure information to a

covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS.—The term "voluntary"—

(i) in the case of any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

[(8) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given those terms in section 2209.]

* * * * * * *

CYBERSECURITY ACT OF 2015

* * * * * * *

SEC. 102. DEFINITIONS

(1) * * *

* * * * * * *

[(4) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

[(5) CYBERSECURITY THREAT.—

[(A) IN GENERAL.—Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

[(B) EXCLUSION.—The term "cybersecurity threat" does not include any action that solely involves a violation of a

consumer term of service or a consumer licensing agreement.

[(6) CYBER THREAT INDICATOR.—The term "cyber threat indicator" means information that is necessary to describe or identify—

[(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

[(B) a method of defeating a security control or exploitation of a security vulnerability;

[(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

[(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

[(E) malicious cyber command and control;

[(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

[(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

[(H) any combination thereof.

[(7) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.]

(4) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(5) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(6) CYBER THREAT INDICATOR.—The term "cyber threat indicator" has the meaning given the term in section 2200 of the Homeland Security Act 13 of 2002.

(7) DEFENSIVE MEASURE.—The term "defensive measure" has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(8) * * *

(9) * * *

[(13) MONITOR.—The term "monitor" means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.**]**

(13) MONITOR.—The term "monitor" has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(14) * * *

(15) * * *

[(16) SECURITY CONTROL.—The term "security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

[(17) SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.**]**

(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

(18) * * *

* * * * * * *

CONSOLIDATED APPROPRIATIONS ACT OF 2016

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

Subtitle B—Federal Cybersecurity Enhancement

SEC. 221. SHORT TITLE.

This subtitle may be cited as the "Federal Cybersecurity Enhancement Act of 2015."

SEC. 222. DEFINITIONS.

(1) * * *

(2) AGENCY INFORMATION SYSTEM.—The term "agency information system" has the meaning given the term in section 2210 of the Homeland Security Act of 2002.

(3) * * *

(4) CYBERSECURITY RISK; INFORMATION SYSTEM.—The terms "cybersecurity risk" and "information system" have the meanings given those terms in section 2209 of the Homeland Security Act of 2002.

SEC. 223. IMPROVED FEDERAL NETWORK SECURITY.

(a) * * *

(b) * * *

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under ⟦section 2213(b)(1)⟧ *section 2213(a)(1)* of the Homeland Security Act of 2002, whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

* * * * * * *

SEC. 226. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section:

(1) AGENCY INFORMATION.—The term "agency information" has the meaning given the term in ⟦section 2213⟧ *section 2200* of the Homeland Security Act of 2002.

(2) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in ⟦section 102⟧ *section 2200 of the Homeland Security Act of 2002*.

(3) * * *

(4) INTRUSION ASSESSMENT PLAN.—The term "intrusion assessment plan" means the plan required under ⟦section 2210(b)(1)⟧ *section 2210(a)(1)* of the Homeland Security Act of 2002.

(5) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—The term "intrusion detection and prevention capabilities" means the capabilities required under section ⟦2213(b)⟧ *section 2213(a)* of the Homeland Security Act of 2002.

* * * * * * *

SEC. 227. TERMINATION.

(a) * * *

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under ⟦section 2213(d)(2)⟧ *section 2213(c)(2)* of the Homeland Security Act of 2002 if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

* * * * * * *

PUBLIC HEALTH SERVICE ACT

* * * * * * *

TITLE XXVIII—NATIONAL ALL HAZARDS PREPAREDNESS FOR PUBLIC HEALTH EMERGENCIES

* * * * * * *

Subtitle B—All Hazards Emergency Preparedness and Response

* * * * * * *

SEC. 2811. COORDINATION OF PREPAREDNESS FOR AND RESPONSE TO ALL HAZARDS PUBLIC HEALTH EMERGENCIES.

(a) * * *
(b) * * *
(1) * * *

* * * * * * *

(4) * * *
(A) * * *

* * * * * * *

(D) Policy Coordination and Strategic Direction.—Provide integrated policy coordination and strategic direction, before, during, and following public health emergencies, with respect to all matters related to Federal public health and medical preparedness and execution and deployment of the Federal response for public health emergencies and incidents covered by the National Response Plan described in section 504(a)(6) of the Homeland Security Act of 2002 (6 U.S.C. 314(a)(6)), or any successor plan; and such Federal responses covered by the National Cybersecurity Incident Response Plan developed under [section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))] *section 2209(c) of the Homeland Security Act of 2002*, including public health emergencies or incidents related to cybersecurity threats that present a threat to national health security.

* * * * * * *

WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2021

* * * * * * *

TITLE XC—HOMELAND SECURITY MATTERS

* * * * * * *

SEC. 9002 SECTOR RISK MANAGEMENT AGENCIES

(a) DEFINITIONS.—In this section:

(1) * * *

* * * * * * *

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "information sharing and analysis organization" has the meaning given that term in section [2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))] *section 2200 of the Homeland Security Act of 2002.*

(6) * * *

(7) SECTOR RISK MANAGEMENT AGENCY. —The term "sector risk management agency" has the meaning [given the term "Sector-Specific Agency" in section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. 651(5))] *given the term in section 2200 of the Homeland Security Act of 2002.*

(b) * * *

(c) * * *

(1) * * *

(2) * * *

(3) * * *

(A) * * *

(B) have the meaning give such term in [section 2201(5)] *section 2200* of the Homeland Security Act of 2002 of the Homeland Security Act of 2002.

(4) * * *

(d) REPORT AND AUDITING.—Not later than two years after the date of the enactment of this Act and every four years thereafter for 12 years, the Comptroller General of the United States 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 on the effectiveness of Sector Risk Management Agencies in carrying out their responsibilities under [section 2215] *2218* of the Homeland Security Act of 2002[, as added by this section].

* * * * * * *

NATIONAL SECURITY ACT OF 1947

* * * * * * *

SEC. 113B. SPECIAL PAY AUTHORITY FOR SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS POSITIONS.

(a) * * *

(b) * * *

(1) * * *

(2) * * *

(3) * * *

(4) LIMITATION ON USE AS COMPARATIVE REFERENCE.—Notwithstanding any other provision of law, special rates of pay and the limitation established under paragraph (1)(B) may not be used as comparative references for the purpose of fixing the rates of basic pay or maximum pay limitations of qualified positions under section 1599f of title 10, United States Code, or [section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147)] *section 2208 of the Homeland Security Act of 2002.*

* * * * * * *

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020

* * * * * * *

SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

(a) * * *

(b) * * *

(1) * * *

(2) * * *

(3) be consistent with the policies and procedures produced under [section 2009(m)] *section 2208(1)* of the Homeland Security Act of 2002 (6 U.S.C. 659(l)).

* * * * * * *

SMALL BUSINESS ACT

* * * * * * *

SEC. 21.

(a) * * *

(8) CYBERSECURITY ASSISTANCE.—

(A) * * *

(B) DEFINITIONS.—In this paragraph, the terms "cybersecurity risk" and "cyber threat indicator" have the meanings given such terms, respectively, under [section 2209(a)] *section 2200* of the Homeland Security Act of 2002.

* * * * * * *

UNITED STATES CODE

TITLE 46

Subchapter I—General

SEC. 70101. DEFINITIONS.

For the purpose of this chapter:

(1) * * *

(2) The term "cybersecurity risk" has the meaning given the term in [section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)] *section 2200 of the Homeland Security Act of 2002*.

* * * * * * *

○