

of cyber capabilities, which is not classified to the Code.

#### CODIFICATION

Section 1548(a) of Pub. L. 117-81, which directed that this section be added at the end of title XXII of the Homeland Security Act of 2002, was executed by adding this section at the end of this part as if the directory language had added the section at the end of subtitle A of title XXII of the Act, to reflect the probable intent of Congress.

#### AMENDMENTS

2022—Subsec. (f). Pub. L. 117-263 added subsec. (f) and struck out former subsec. (f) which defined cybersecurity risk, industrial control system, and information system.

### § 665j. Ransomware threat mitigation activities

#### (a) Joint Ransomware Task Force

##### (1) In general

Not later than 180 days after March 15, 2022, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

##### (2) Composition

The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

##### (3) Responsibilities

The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify<sup>1</sup> metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

<sup>1</sup> So in original.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

#### (b) Rule of construction

Nothing in this section shall be construed to provide any additional authority to any Federal agency.

(Pub. L. 117-103, div. Y, §106, Mar. 15, 2022, 136 Stat. 1056.)

#### Editorial Notes

##### CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

#### Statutory Notes and Related Subsidiaries

##### DEFINITIONS

Pub. L. 117-103, div. Y, §102, Mar. 15, 2022, 136 Stat. 1038, provided that: “In this division [see Short Title of 2022 Amendment note set out under section 101 of this title]:

“(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ‘covered cyber incident’, ‘covered entity’, ‘cyber incident’, ‘information system’, ‘ransom payment’, ‘ransomware attack’, and ‘security vulnerability’ have the meanings given those terms in section 2240 of the Homeland Security Act of 2002 [6 U.S.C. 681], as added by section 103 of this division [see also 6 U.S.C. 650].

“(2) DIRECTOR.—The term ‘Director’ means the Director of the Cybersecurity and Infrastructure Security Agency.”

### § 665k. Federal Clearinghouse on School Safety Evidence-based Practices

#### (a) Establishment

##### (1) In general

The Secretary, in coordination with the Secretary of Education, the Attorney General, and the Secretary of Health and Human Services, shall establish a Federal Clearinghouse on School Safety Evidence-based Practices (in this section referred to as the “Clearinghouse”) within the Department.

##### (2) Purpose

The Clearinghouse shall serve as a Federal resource to identify and publish online through SchoolSafety.gov, or any successor website, evidence-based practices and recommendations to improve school safety for use by State and local educational agencies, institutions of higher education, State and local law enforcement agencies, health professionals, and the general public.

##### (3) Personnel

##### (A) Assignments

The Clearinghouse shall be assigned such personnel and resources as the Secretary