vate organization to assist the government or organization in establishing a program of training to identify human trafficking, upon request from the government or organization.

(Pub. L. 114–22, title IX, § 904, May 29, 2015, 129 Stat. 266.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§ 645. Victim protection training for the Department of Homeland Security

(a) Directive to DHS law enforcement officials and task forces

(1) In general

Not later than 180 days after December 21, 2018, the Secretary shall issue a directive to—

(A) all Federal law enforcement officers and relevant personnel employed by the Department who may be involved in the investigation of human trafficking offenses; and

(B) members of all task forces led by the Department that participate in the investigation of human trafficking offenses.

(2) Required instructions

The directive required to be issued under paragraph (1) shall include instructions on—

(A) the investigation of individuals who patronize or solicit human trafficking victims as being engaged in severe trafficking in persons and how such individuals should be investigated for their roles in severe trafficking in persons; and

(B) how victims of sex or labor trafficking often engage in criminal acts as a direct result of severe trafficking in persons and such individuals are victims of a crime and affirmative measures should be taken to avoid arresting, charging, or prosecuting such individuals for any offense that is the direct result of their victimization.

(b) Victim screening protocol

(1) In general

Not later than 180 days after December 21, 2018, the Secretary shall issue a screening protocol for use during all anti-trafficking law enforcement operations in which the Department is involved.

(2) Requirements

The protocol required to be issued under paragraph (1) shall—

(A) require the individual screening of all adults and children who are suspected of engaging in commercial sex acts, child labor that is a violation of law, or work in violation of labor standards to determine whether each individual screened is a victim of human trafficking;

(B) require affirmative measures to avoid arresting, charging, or prosecuting human trafficking victims for any offense that is the direct result of their victimization;

(C) be developed in consultation with relevant interagency partners and nongovernmental organizations that specialize in the prevention of human trafficking or in the identification and support of victims of human trafficking and survivors of human trafficking; and

(D) include—

(i) procedures and practices to ensure that the screening process minimizes trauma or revictimization of the person being screened; and

(ii) guidelines on assisting victims of human trafficking in identifying and receiving restorative services.

(c) Mandatory training

The training described in sections 642 and 644 of this title shall include training necessary to implement—

(1) the directive required under subsection (a); and

(2) the protocol required under subsection (b).

(Pub. L. 114–22, title IX, § 906, as added Pub. L. 115–392, § 5(a), Dec. 21, 2018, 132 Stat. 5252.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Justice for Victims of Trafficking Act of 2015, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

§ 645a. Human trafficking assessment

Not later than 1 year after December 21, 2018, and annually thereafter, the Executive Associate Director of Homeland Security Investigations shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate, and the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives a report on human trafficking investigations undertaken by Homeland Security Investigations that includes—

(1) the number of confirmed human trafficking investigations by category, including labor trafficking, sex trafficking, and transnational and domestic human trafficking;

(2) the number of victims by category, including—

(A) whether the victim is a victim of sex trafficking or a victim of labor trafficking; and

(B) whether the victim is a minor or an adult; and

(3) an analysis of the data described in paragraphs (1) and (2) and other data available to Homeland Security Investigations that indicates any general human trafficking or investigatory trends.

(Pub. L. 115–393, title IV, § 403, Dec. 21, 2018, 132 Stat. 5275.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Trafficking Victims Protection Act of 2017, and not as part of the

Homeland Security Act of 2002 which comprises this chapter.

SUBCHAPTER XVIII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

§ 650. Definitions

Except as otherwise specifically provided, in this subchapter:

(1) Agency

The term ''Agency'' means the Cybersecurity and Infrastructure Security Agency.

(2) Appropriate congressional committees

The term ''appropriate congressional committees'' 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.

(3) Cloud service provider

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

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) 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 infor-