(2) Covered intelligence assistance

The term ''covered intelligence assistance'' has the meaning given that term in section 5703.

(Pub. L. 116–92, div. E, title LVII, § 5717, Dec. 20, 2019, 133 Stat. 2174.)

Editorial Notes

REFERENCES IN TEXT

Section 5703, referred to in subsecs. (a) and (c)(2), is section 5703 of Pub. L. 116–92, which is set out as a note below.

Statutory Notes and Related Subsidiaries

STUDY ON ROLE OF RETIRED AND FORMER PERSONNEL OF INTELLIGENCE COMMUNITY WITH RESPECT TO CERTAIN FOREIGN INTELLIGENCE OPERATIONS

Pub. L. 116–92, div. E, title LVII, § 5703, Dec. 20, 2019, 133 Stat. 2162, provided that:

''(a) STUDY.—The Director of National Intelligence shall conduct a study on former intelligence personnel providing covered intelligence assistance.

''(b) ELEMENTS.—The study under subsection (a) shall include the following:

''(1) An identification of, and discussion of the effectiveness of, existing laws, policies, procedures, and other measures relevant to the ability of elements of the intelligence community [see Definitions note below] to prevent former intelligence personnel from providing covered intelligence assistance—

''(A) without proper authorization; or

''(B) in a manner that would violate legal or policy controls if the personnel performed such assistance while working for the United States Government; and

''(2) Make recommendations for such legislative, regulatory, policy, or other changes as may be necessary to ensure that the United States consistently meets the objectives described in paragraph (1).

''(c) REPORT AND PLAN.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Director shall submit to the congressional intelligence committees [see Definitions note below], the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives—

''(1) a report on the findings of the Director with respect to each element of the study under subsection (a); and

''(2) a plan to implement any recommendations made by the Director that the Director may implement without changes to Federal law.

''(d) FORM.—The report and plan under subsection (c) may be submitted in classified form.

''(e) DEFINITIONS.—In this section:

''(1) COVERED INTELLIGENCE ASSISTANCE.—The term 'covered intelligence assistance' means assistance—

''(A) provided by former intelligence personnel directly to, or for the benefit of, the government of a foreign country or indirectly to, or for the benefit of, such a government through a company or other entity; and

''(B) that relates to intelligence, military, or law enforcement activities of a foreign country, including with respect to operations that involve abuses of human rights, violations of the laws of the United States, or infringements on the privacy rights of United States persons.

''(2) FORMER INTELLIGENCE PERSONNEL.—The term 'former intelligence personnel' means retired or former personnel of the intelligence community, including civilian employees of elements of the intelligence community, members of the Armed Forces, and contractors of elements of the intelligence community.''

DEFINITIONS

For definitions of ''intelligence community'' and ''congressional intelligence committees'', referred to in text, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3334d. Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack

(a) Definitions

In this section:

(1) Personal accounts

The term ''personal accounts'' means accounts for online and telecommunications services, including telephone, residential internet access, email, text and multimedia messaging, cloud computing, social media, health care, and financial services, used by personnel of the intelligence community outside of the scope of their employment with elements of the intelligence community.

(2) Personal technology devices

The term ''personal technology devices'' means technology devices used by personnel of the intelligence community outside of the scope of their employment with elements of the intelligence community, including networks to which such devices connect.

(b) Authority to provide cyber protection support

(1) In general

Subject to a determination by the Director of National Intelligence, the Director may provide cyber protection support for the personal technology devices and personal accounts of the personnel described in paragraph (2).

(2) At-risk personnel

The personnel described in this paragraph are personnel of the intelligence community—

(A) who the Director determines to be highly vulnerable to cyber attacks and hostile information collection activities because of the positions occupied by such personnel in the intelligence community; and

(B) whose personal technology devices or personal accounts are highly vulnerable to cyber attacks and hostile information collection activities.

(c) Nature of cyber protection support

Subject to the availability of resources, the cyber protection support provided to personnel under subsection (b) may include training, advice, assistance, and other services relating to cyber attacks and hostile information collection activities.

(d) Limitation on support

Nothing in this section shall be construed—

(1) to encourage personnel of the intelligence community to use personal technology devices for official business; or

(2) to authorize cyber protection support for senior intelligence community personnel using personal devices, networks, and personal accounts in an official capacity.

(e) Report

Not later than 180 days after December 20, 2019, the Director shall submit to the congres-

sional intelligence committees a report on the provision of cyber protection support under subsection (b). The report shall include—

(1) a description of the methodology used to make the determination under subsection (b)(2); and

(2) guidance for the use of cyber protection support and tracking of support requests for personnel receiving cyber protection support under subsection (b).

(Pub. L. 116–92, div. E, title LXIII, § 6308, Dec. 20, 2019, 133 Stat. 2189.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of ''intelligence community'' and ''congressional intelligence committees'', referred to in text, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3334e. Enhanced procurement authority to manage supply chain risk

(a) Definitions

In this section:

(1) Covered agency

The term ''covered agency'' means any element of the intelligence community other than an element within the Department of Defense.

(2) Covered item of supply

The term ''covered item of supply'' means an item of information technology (as that term is defined in section 11101 of title 40) that is purchased for inclusion in a covered system, and the loss of integrity of which could result in a supply chain risk for a covered system.

(3) Covered procurement

The term ''covered procurement'' means—

(A) a source selection for a covered system or a covered item of supply involving either a performance specification, as provided in section 3306(a)(3)(B) of title 41, or an evaluation factor, as provided in section 3306(b)(1) of such title, relating to supply chain risk;

(B) the consideration of proposals for and issuance of a task or delivery order for a covered system or a covered item of supply, as provided in section 4106(d)(3) of title 41, where the task or delivery order contract concerned includes a contract clause establishing a requirement relating to supply chain risk; or

(C) any contract action involving a contract for a covered system or a covered item of supply where such contract includes a clause establishing requirements relating to supply chain risk.

(4) Covered procurement action

The term ''covered procurement action'' means any of the following actions, if the action takes place in the course of conducting a covered procurement:

(A) The exclusion of a source that fails to meet qualifications standards established in accordance with the requirements of section 3311 of title 41 for the purpose of reducing supply chain risk in the acquisition of covered systems.

(B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

(C) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

(5) Covered system

The term ''covered system'' means a national security system, as that term is defined in section 3542(b)[1] of title 44.

(6) Supply chain risk

The term ''supply chain risk'' means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(b) Authority

Subject to subsection (c) and in consultation with the Director of National Intelligence, the head of a covered agency may, in conducting intelligence and intelligence-related activities—

(1) carry out a covered procurement action; and

(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information relating to the basis for carrying out a covered procurement action.

(c) Determination and notification

The head of a covered agency may exercise the authority provided in subsection (b) only after—

(1) any appropriate consultation with procurement or other relevant officials of the covered agency;

(2) making a determination in writing, which may be in classified form, that—

(A) use of the authority in subsection (b)(1) is necessary to protect national security by reducing supply chain risk;

(B) less intrusive measures are not reasonably available to reduce such supply chain risk; and

(C) in a case where the head of the covered agency plans to limit disclosure of information under subsection (b)(2), the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information;

(3) notifying the Director of National Intelligence that there is a significant supply chain risk to the covered system concerned, unless the head of the covered agency making the determination is the Director of National Intelligence; and

(4) providing a notice, which may be in classified form, of the determination made under paragraph (2) to the congressional intelligence

[1] See References in Text note below.