this title. For complete classification of this Act to the Code, see Short Title note set out under section 2151 of this title and Tables.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of ''Secretary'' and ''appropriate congressional committees'' as used in this section, see section 6002 of Pub. L. 118–31, set out as a note under section 2651 of this title.

§ 10308. Cyber protection support for personnel of the Department of State in positions highly vulnerable to cyber attack

(a) Definitions

In this section:

(1) At-risk personnel

The term ''at-risk personnel'' means personnel of the Department—

(A) whom the Secretary determines to be highly vulnerable to cyber attacks and hostile information collection activities because of their positions in the Department; and

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

(2) 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 Department personnel outside of the scope of their employment with the Department.

(3) Personal technology devices

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

(b) Requirement to provide cyber protection support

The Secretary, in consultation with the Secretary of Homeland Security and the Director of National Intelligence, as appropriate—

(1) shall offer cyber protection support for the personal technology devices and personal accounts of at-risk personnel; and

(2) may provide the support described in paragraph (1) to any Department personnel who request such support.

(c) Nature of cyber protection support

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

(d) Privacy protections for personal devices

The Department is prohibited pursuant to this section from accessing or retrieving any information from any personal technology device or personal account of Department employees unless—

(1) access or information retrieval is necessary for carrying out the cyber protection support specified in this section; and

(2) the Department has received explicit consent from the employee to access a personal technology device or personal account prior to each time such device or account is accessed.

(e) Rule of construction

Nothing in this section may be construed—

(1) to encourage Department personnel to use personal technology devices for official business; or

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

(f) Report

(1) In general

Not later than 180 days after December 22, 2023, the Secretary shall submit to the appropriate committees of Congress a report regarding the provision of cyber protection support pursuant to subsection (b), which shall include—

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

(B) guidance for the use of cyber protection support and tracking of support requests for personnel receiving cyber protection support pursuant to subsection (b).

(2) Appropriate committees of Congress defined

In this subsection, the term ''appropriate committees of Congress'' means—

(A) the appropriate congressional committees;

(B) the Select Committee on Intelligence and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Permanent Select Committee on Intelligence and the Committee on Oversight and Accountability of the House of Representatives.

(Pub. L. 118–31, div. F, title LXIII, § 6308, Dec. 22, 2023, 137 Stat. 993.)

Statutory Notes and Related Subsidiaries

MEASURES TO PROTECT DEPARTMENT DEVICES FROM THE PROLIFERATION AND USE OF FOREIGN COMMERCIAL SPYWARE

Pub. L. 118–159, div. G, title LXXIII, § 7302, Dec. 23, 2024, 138 Stat. 2541, provided that:

''(a) DEFINITIONS.—In this section:

''(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' means—

''(A) the Committee on Foreign Relations, the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, and the Committee on Armed Services of the Senate; and

''(B) the Committee on Foreign Affairs, the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Armed Services of the House of Representatives.

''(2) COVERED DEVICE.—The term 'covered device' means any electronic mobile device, including smartphones, tablet computing devices, or laptop

computing device, that is issued by the Department for official use.

''(3) FOREIGN COMMERCIAL SPYWARE; SPYWARE.—The terms 'foreign commercial spyware' and 'spyware' have the meanings given those terms in section 1102A of the National Security Act of 1947 (50 U.S.C. 3232a).

''(b) PROTECTION OF COVERED DEVICES.—

''(1) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act [Dec. 23, 2024], the Secretary [of State] shall, in consultation with the relevant agencies—

''(A) issue standards, guidance, best practices, and policies for Department [of State] and USAID [United States Agency for International Development] personnel to protect covered devices from being compromised by foreign commercial spyware;

''(B) survey the processes used by the Department and USAID to identify and catalog instances where a covered device was compromised by foreign commercial spyware over the prior 2 years and it is reasonably expected to have resulted in an unauthorized disclosure of sensitive information; and

''(C) submit to the appropriate committees of Congress a report on the measures in place to identify and catalog instances of such compromises for covered devices by foreign commercial spyware, which may be submitted in classified form.

''(2) NOTIFICATIONS.—Not later than 60 days after the date on which the Department becomes aware that a covered device was seriously compromised by foreign commercial spyware, the Secretary, in coordination with relevant agencies, shall notify the appropriate committees of Congress of the facts concerning such targeting or compromise, including—

''(A) the location of the personnel whose covered device was compromised;

''(B) the number of covered devices compromised;

''(C) an assessment by the Secretary of the damage to the national security of the United States resulting from any loss of data or sensitive information; and

''(D) an assessment by the Secretary of any foreign government or foreign organization or entity, and, to the extent possible, the foreign individuals, who directed and benefitted from any information acquired from the compromise.

''(3) ANNUAL REPORT.—Not later than one year after the date of the enactment of this Act, and annually thereafter for 5 years, the Secretary, in coordination with relevant agencies, shall submit to the appropriate committees of Congress, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives a report regarding any covered device that was compromised by foreign commercial spyware, including the information described in subparagraphs (A) through (D) of paragraph (2).''

DEFINITIONS

For definitions of ''Department'', ''Secretary'', and ''appropriate congressional committees'' as used in this section, see section 6002 of Pub. L. 118–31, set out as a note under section 2651 of this title.

CHAPTER 111—AUSTRALIA, UNITED KINGDOM, AND UNITED STATES (AUKUS) SECURITY PARTNERSHIP

§ 10401. Definitions

In this chapter:

(1) Appropriate congressional committees

Except as otherwise provided, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations and the Committee on Armed Services of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Armed Services of the House of Representatives.

(2) AUKUS partnership

(A) In general

The term ''AUKUS partnership'' means the enhanced trilateral security partnership between Australia, the United Kingdom, and the United States announced in September 2021.

(B) Pillars

The AUKUS partnership includes the following two pillars:

(i) Pillar One is focused on developing a pathway for Australia to acquire conventionally armed, nuclear-powered submarines.

(ii) Pillar Two is focused on enhancing trilateral collaboration on advanced defense capabilities, including hypersonic and counter hypersonic capabilities, quantum technologies, undersea technologies, and artificial intelligence.

(3) International Traffic in Arms Regulations

The term ''International Traffic in Arms Regulations'' means subchapter M of chapter I of title 22, Code of Federal Regulations (or successor regulations).

(Pub. L. 118–31, div. A, title XIII, §1321, Dec. 22, 2023, 137 Stat. 501.)

Statutory Notes and Related Subsidiaries

SHORT TITLE

Pub. L. 118–31, div. A, title XIII, §1351, Dec. 22, 2023, 137 Stat. 514, provided that: ''This part [part 3