the date of the enactment of this Act,'' in introductory provisions and '', civil liberties, and civil rights'' for ''and civil liberties'' in pars. (1) and (2).

§ 3241. Biennial reports on foreign biological threats

(a) Reports

On a biennial basis until the date that is 10 years after March 15, 2022, the Director of National Intelligence shall submit to the congressional intelligence committees a comprehensive report on the activities, prioritization, and responsibilities of the intelligence community with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country.

(b) Matters included

Each report under subsection (a) shall include, with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country, the following:

(1) A detailed description of all activities relating to such threats undertaken by each element of the intelligence community, and an assessment of any gaps in such activities.

(2) A detailed description of all duties and responsibilities relating to such threats explicitly authorized or otherwise assigned, exclusively or jointly, to each element of the intelligence community, and an assessment of any identified gaps in such duties or responsibilities.

(3) A description of the coordination among the relevant elements of the intelligence community with respect to the activities specified in paragraph (1) and the duties and responsibilities specified in paragraph (2).

(4) An inventory of the strategies, plans, policies, and interagency agreements of the intelligence community relating to the collection, monitoring, analysis, mitigation, and attribution of such threats, and an assessment of any identified gaps therein.

(5) A description of the coordination and interactions among the relevant elements of the intelligence community and non-intelligence community partners.

(6) An assessment of foreign malign influence efforts relating to such threats, including any foreign academics engaged in such efforts, and a description of how the intelligence community contributes to efforts by non-intelligence community partners to counter such foreign malign influence.

(c) Form

Each report submitted under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

(d) Definitions

In this section:

(1) Covered country

The term ''covered country'' means—

(A) China;

(B) Iran;

(C) North Korea;

(D) Russia; and

(E) any other foreign country—

(i) from which the Director of National Intelligence determines a biological threat emanates; or

(ii) that the Director determines has a known history of, or has been assessed as having conditions present for, infectious disease outbreaks or epidemics.

(2) Foreign biological threat

The term ''foreign biological threat'' means biological warfare, bioterrorism, naturally occurring infectious diseases, or accidental exposures to biological materials, without regard to whether the threat originates from a state actor, a non-state actor, natural conditions, or an undetermined source.

(3) Foreign malign influence

The term ''foreign malign influence'' has the meaning given such term in section 3059(e)[1] of this title.

(4) Non-intelligence community partner

The term ''non-intelligence community partner'' means a Federal department or agency that is not an element of the intelligence community.

(July 26, 1947, ch. 343, title XI, § 1111, as added Pub. L. 117–103, div. X, title VIII, § 821(a), Mar. 15, 2022, 136 Stat. 1019.)

Editorial Notes

REFERENCES IN TEXT

Section 3059(e) of this title, referred to in subsec. (d)(3), was redesignated as section 3059(f) of this title by Pub. L. 117–263, div. F, title LXIII, §6307(b)(1), Dec. 23, 2022, 136 Stat. 3505.

Statutory Notes and Related Subsidiaries

FIRST REPORT

Pub. L. 117–103, div. X, title VIII, § 821(b), Mar. 15, 2022, 136 Stat. 1020, provided that: ''Not later than 120 days after the date of the enactment of this Act [Mar. 15, 2022], the Director of National Intelligence shall submit to the congressional intelligence committees the first report required under section 1111 of the National Security Act of 1947 [50 U.S.C. 3241], as added by subsection (a).''

[For definition of ''congressional intelligence committees'' as used in section 821(b) of div. X of Pub. L. 117–103, set out above, see section 2 of div. X of Pub. L. 117–103, set out as a note under section 3003 of this title.]

§ 3242. Annual reports on certain cyber vulnerabilities procured by intelligence community and foreign commercial providers of cyber vulnerabilities

(a) Annual reports

On an annual basis through 2026, the Director of the Central Intelligence Agency and the Director of the National Security Agency, in coordination with the Director of National Intelligence, shall jointly submit to the congressional intelligence committees a report containing information on foreign commercial providers and the cyber vulnerabilities procured by the intelligence community through foreign commercial providers.

[1] See References in Text note below.

(b) Elements

Each report under subsection (a) shall include, with respect to the period covered by the report, the following:

(1) A description of each cyber vulnerability procured through a foreign commercial provider, including—

(A) a description of the vulnerability;

(B) the date of the procurement;

(C) whether the procurement consisted of only that vulnerability or included other vulnerabilities;

(D) the cost of the procurement;

(E) the identity of the commercial provider and, if the commercial provider was not the original supplier of the vulnerability, a description of the original supplier;

(F) the country of origin of the vulnerability; and

(G) an assessment of the ability of the intelligence community to use the vulnerability, including whether such use will be operational or for research and development, and the approximate timeline for such use.

(2) An assessment of foreign commercial providers that—

(A) pose a significant threat to the national security of the United States; or

(B) have provided cyber vulnerabilities to any foreign government that—

(i) has used the cyber vulnerabilities to target United States persons, the United States Government, journalists, or dissidents; or

(ii) has an established pattern or practice of violating human rights or suppressing dissent.

(3) An assessment of whether the intelligence community has conducted business with the foreign commercial providers identified under paragraph (2) during the 5-year period preceding the date of the report.

(c) Form

Each report under subsection (a) may be submitted in classified form.

(d) Definitions

In this section:

(1) Commercial provider

The term ''commercial provider'' means any person that sells, or acts as a broker, for a cyber vulnerability.

(2) Cyber vulnerability

The term ''cyber vulnerability'' means any tool, exploit, vulnerability, or code that is intended to compromise a device, network, or system, including such a tool, exploit, vulnerability, or code procured by the intelligence community for purposes of research and development.

(July 26, 1947, ch. 343, title XI, §1112, as added Pub. L. 117–103, div. X, title VIII, §822(a), Mar. 15, 2022, 136 Stat. 1020.)

Statutory Notes and Related Subsidiaries

FIRST REPORT

Pub. L. 117–103, div. X, title VIII, §822(b), Mar. 15, 2022, 136 Stat. 1021, provided that: ''Not later than 90 days after the date of the enactment of this Act [Mar. 15, 2022], the Director of the Central Intelligence Agency and the Director of the National Security Agency shall jointly submit the first report required under section 1112 of the National Security Act of 1947 [50 U.S.C. 3242], as added by subsection (a).''

§ 3243. Periodic reports on technology strategy of intelligence community

(a) Reports

On a basis that is not less frequent than once every 4 years, the Director of National Intelligence, in coordination with the Director of the Office of Science and Technology Policy, the Secretary of Commerce, and the heads of such other agencies as the Director considers appropriate, shall submit to the congressional intelligence committees a comprehensive report on the technology strategy of the intelligence community, which shall be designed to support the maintenance of the leadership of the United States in critical and emerging technologies essential to the national security of the United States.

(b) Elements

Each report submitted under subsection (a) shall include the following:

(1) An assessment of technologies critical to the national security of the United States, particularly those technologies with respect to which foreign countries that are adversarial to the United States have or are poised to match or surpass the technology leadership of the United States.

(2) A review of current technology policies of the intelligence community, including long-term goals.

(3) An identification of sectors and supply chains the Director determines to be of the greatest strategic importance to national security.

(4) An identification of opportunities to protect the leadership of the United States, and the allies and partners of the United States, in critical technologies, including through targeted export controls, investment screening, and counterintelligence activities.

(5) An identification of research and development areas the Director determines critical to the national security of the United States, including areas in which the private sector does not focus.

(6) Recommendations for growing talent in key critical and emerging technologies and enhancing the ability of the intelligence community to recruit and retain individuals with critical skills relating to such technologies.

(7) An identification of opportunities to improve the leadership of the United States in critical technologies, including opportunities to develop international partnerships to reinforce domestic policy actions, develop new markets, engage in collaborative research, and maintain an international environment that reflects the values of the United States and protects the interests of the United States.

(8) A technology annex to establish an approach for the identification, prioritization, development, and fielding of emerging technologies critical to the mission of the intelligence community.