

(9) Such other information as the Director determines may be necessary to inform Congress on matters relating to the technology strategy of the intelligence community and related implications for the national security of the United States.

(c) Form of annex

Each annex submitted under subsection (b)(8) may be submitted in classified form.

(July 26, 1947, ch. 343, title XI, §1113, as added Pub. L. 117–103, div. X, title VIII, §823(a), Mar. 15, 2022, 136 Stat. 1021.)

Statutory Notes and Related Subsidiaries

FIRST REPORT

Pub. L. 117–103, div. X, title VIII, §823(b), Mar. 15, 2022, 136 Stat. 1022, provided that: “Not later than 1 year 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 1113 of the National Security Act of 1947 [50 U.S.C. 3243], as added by subsection (a).”

[For definition of “congressional intelligence committees” as used in section 823(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.]

§ 3244. Annual report on reporting requirements

(a) Annual report required

Not later than March 1 of each fiscal year, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report detailing all congressionally mandated reporting requirements applicable to the Office of the Director of National Intelligence for the upcoming fiscal year.

(b) Contents

Each report submitted pursuant to subsection (a) shall include, for the fiscal year covered by the report and for each congressionally mandated reporting requirement detailed in the report:

- (1) A description of the reporting requirement.
- (2) A citation to the provision of law (or other source of congressional directive) imposing the reporting requirement.
- (3) Whether the reporting requirement is recurring, conditional, or subject to a termination provision.
- (4) Whether the Director recommends repealing or modifying the requirement.

(c) Form

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

(July 26, 1947, ch. 343, title XI, §1114, as added Pub. L. 118–31, div. G, title III, §7314(a), Dec. 22, 2023, 137 Stat. 1031; amended Pub. L. 118–159, div. F, title LXIX, §6902(a)(5), Dec. 23, 2024, 138 Stat. 2517.)

Editorial Notes

AMENDMENTS

2024—Subsec. (a). Pub. L. 118–159 inserted “the” before “Office of the Director”.

**CHAPTER 45—MISCELLANEOUS
INTELLIGENCE COMMUNITY AUTHORITIES**

SUBCHAPTER I—BUDGET AND OVERSIGHT

- | | |
|--------|---|
| Sec. | |
| 3301. | Multiyear national intelligence program. |
| 3302. | Identification of constituent components of base intelligence budget. |
| 3303. | Construction of intelligence community facilities; Presidential authorization. |
| 3304. | Limitation on construction of facilities to be used primarily by intelligence community. |
| 3305. | Exhibits for inclusion with budget justification books. |
| 3306. | Availability to public of certain intelligence funding information. |
| 3307. | Communications with the Committees on Armed Services of the Senate and the House of Representatives. |
| 3308. | Information access by the Comptroller General of the United States. |
| 3308a. | Provision of certain information to Government Accountability Office by National Reconnaissance Office. |
| 3309. | Notification of establishment of advisory committee. |
| 3310. | Annual report on United States security arrangements and commitments with other nations. |
| 3311. | Submittal to Congress by heads of elements of intelligence community of plans for orderly shutdown in event of absence of appropriations. |
| 3312. | Repealed. |
| 3313. | Notification of memoranda of understanding. |
| 3314. | Report on national security systems. |
| 3315. | Repealed. |
| 3316. | Submission of intelligence community policies. |
| 3316a. | Reports on intelligence community participation in vulnerabilities equities process of Federal Government. |
| 3316b. | Continuity of operations plans for certain elements of the intelligence community in the case of a national emergency. |
| 3316c. | Development of definitions for certain terms relating to intelligence. |
| | SUBCHAPTER II—PERSONNEL AND ADMINISTRATIVE AUTHORITIES |
| 3321. | National Intelligence Reserve Corps. |
| 3322. | Additional education and training requirements. |
| 3323. | Eligibility for incentive awards. |
| 3324. | Prohibition on using journalists as agents or assets. |
| 3325. | Reaffirmation of longstanding prohibition against drug trafficking by employees of the intelligence community. |
| 3326. | Limitation of expenditure of funds appropriated for Department of Defense intelligence programs. |
| 3327. | Limitation on transfer of funds between CIA and Department of Defense; congressional notification required. |
| 3328. | Study or plan of surrender; use of appropriations. |
| 3329. | Intelligence community contracting. |
| 3330. | Reports to the intelligence community on penetrations of networks and information systems of certain contractors. |
| 3331. | Management of intelligence community personnel. |
| 3332. | Guidance and reporting requirement regarding the interactions between the intelligence community and entertainment industry. |
| 3333. | Joint facilities certification. |
| 3334. | Intelligence community public-private talent exchange. |

- Sec.
3334a. Transfer of National Intelligence University to the Office of the Director of National Intelligence.
- 3334b. Collection, analysis, and dissemination of workforce data.
- 3334c. Assessment of homeland security vulnerabilities associated with certain retired and former personnel of the intelligence community.
- 3334d. Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack.
- 3334e. Enhanced procurement authority to manage supply chain risk.
- 3334f. Congressional notification of designation of covered intelligence officer as persona non grata.
- 3334g. Reports on intelligence community loan repayment and related programs.
- 3334h. Data collection on attrition in intelligence community.
- 3334i. Seedling investment in next-generation microelectronics in support of artificial intelligence.
- 3334j. Access to certain facilities of United States Government for assessment of anomalous health conditions.
- 3334k. Report on protocols for certain intelligence community employees and dependents.
- 3334l. Oversight of Defense Intelligence Agency culture.
- 3334m. Additional responsibilities of Director of National Intelligence for artificial intelligence policies, standards, and guidance for the intelligence community.
- 3334n. Certification relating to information technology and software systems.
- 3334o. Requirements and report on workforce needs of intelligence community relating to science, technology, engineering, and math, and related areas.
- 3334p. Increased intelligence-related engineering, research, and development capabilities of minority institutions.
- 3334q. Detail of individuals from intelligence community to Department of Commerce.
- 3334r. Designation of a chief technology officer within certain elements of the intelligence community.
- 3334s. Programs for next-generation microelectronics in support of artificial intelligence.
- 3334t. Program for beyond 5G.
- 3334u. Notification of referral to Department of Justice.

SUBCHAPTER III—SECURITY CLEARANCES AND CLASSIFIED INFORMATION

3341. Security clearances.
3342. Security clearances for transition team members.
3343. Security clearances; limitations.
3344. Classification training program.
- 3344a. Training to promote sensible classification.
3345. Limitation on handling, retention, and storage of certain classified materials by the Department of State.
3346. Compilation and organization of previously declassified records.
3347. Secrecy agreements used in intelligence activities.
3348. Reports relating to certain special access programs and similar programs.
- 3348a. Congressional oversight of sensitive programs not covered by other provisions of law.
3349. Notification regarding the authorized public disclosure of national intelligence.
3350. Maximum amount charged for declassification reviews.
- 3350a. Promoting efficient declassification review.

- Sec.
3351. Improving quality of information in background investigation request packages.
- 3351a. Making certain policies and execution plans relating to personnel clearances available to industry partners.
- 3351b. Limitations on determinations regarding certain security classifications.
3352. Definitions.
- 3352a. Reports and plans relating to security clearances and background investigations.
- 3352b. Improving the process for security clearances.
- 3352c. Goals for promptness of determinations regarding security clearances.
- 3352d. Reports on reciprocity for security clearances inside of departments and agencies.
- 3352e. Periodic report on positions in the intelligence community that can be conducted without access to classified information, networks, or facilities.
- 3352f. Information-sharing program for positions of trust and security clearances.
- 3352g. Requirement to authorize additional security clearances for certain contractors.
- 3352h. Timeliness standard for rendering determinations of trust for personnel vetting.

SUBCHAPTER III-A—PUBLIC INTEREST DECLASSIFICATIONS

3355. Findings.
- 3355a. Public Interest Declassification Board.
- 3355b. Identification, collection, and review for declassification of information of archival value or extraordinary public interest.
- 3355c. Protection of national security information and other information.
- 3355d. Standards and procedures.
- 3355e. Judicial review.
- 3355f. Funding.
- 3355g. Definitions.

SUBCHAPTER IV—COLLECTION, ANALYSIS, AND SHARING OF INTELLIGENCE

3361. National Virtual Translation Center.
3362. Foreign Terrorist Asset Tracking Center.
3363. Terrorist Identification Classification System.
3364. Assignment of responsibilities relating to analytic integrity.
3365. Foreign intelligence information.
3366. Authorities of heads of other departments and agencies.
3367. Requirement for efficient use by intelligence community of open-source intelligence.
3368. Assistance for governmental entities and private entities in recognizing online violent extremist content.
3369. Cooperative actions to detect and counter foreign influence operations.
- 3369a. Report on deepfake technology, foreign weaponization of deepfakes, and related notifications.
- 3369b. Oversight of foreign influence in academia.
- 3369c. Notification of an active measures campaign.
- 3369d. Committee to counter active measures by the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state to exert covert influence over peoples and governments.
3370. Supply Chain and Counterintelligence Risk Management Task Force.
- 3370a. Repealed.
- 3370b. Collaboration between intelligence community and Department of Commerce to counter foreign commercial threats.
3371. Required counterintelligence assessments, briefings, notifications, and reports.
- 3371a. Assessment of foreign intelligence threats to Federal elections.

- Sec.
3371b. Information sharing with State election officials.
3371c. Notification of significant foreign cyber intrusions and active measures campaigns directed at elections for Federal offices.
3371d. Designation of counterintelligence officer to lead election security matters.
3372. Monitoring mineral investments under Belt and Road Initiative of People's Republic of China.
3373. Establishment of All-domain Anomaly Resolution Office.
3373a. Support for and oversight of Unidentified Aerial Phenomena Task Force.
3373b. Unidentified anomalous phenomena reporting procedures.

SUBCHAPTER V—MANAGEMENT OF COUNTERINTELLIGENCE ACTIVITIES

3381. Coordination of counterintelligence activities.
3382. Director of the National Counterintelligence and Security Center.
3383. National Counterintelligence and Security Center.
3384. Intelligence Community Counterintelligence Office at the Department of Agriculture.
3385. Benjamin Tallmadge Institute as primary Central Intelligence Agency entity for education and training in counterintelligence.

SUBCHAPTER I—BUDGET AND OVERSIGHT

§ 3301. Multiyear national intelligence program

(a) Annual submission of multiyear national intelligence program

The Director of National Intelligence shall submit to the congressional committees specified in subsection (d) each year a multiyear national intelligence program plan reflecting the estimated expenditures and proposed appropriations required to support that program. Any such multiyear national intelligence program plan shall cover the fiscal year with respect to which the budget is submitted and at least four succeeding fiscal years.

(b) Time of submission

The Director of National Intelligence shall submit the report required by subsection (a) each year at or about the same time that the budget is submitted to Congress pursuant to section 1105(a) of title 31.

(c) Consistency with budget estimates

The Director of National Intelligence and the Secretary of Defense shall ensure that the estimates referred to in subsection (a) are consistent with the budget estimates submitted to Congress pursuant to section 1105(a) of title 31 for the fiscal year concerned and with the estimated expenditures and proposed appropriations for the future-years defense program submitted pursuant to section 221 of title 10.

(d) Specified congressional committees

The congressional committees referred to in subsection (a) are the following:

- (1) The Committee on Armed Services, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate.
- (2) The Committee on Armed Services, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives.

(Pub. L. 101–510, div. A, title XIV, §1403, Nov. 5, 1990, 104 Stat. 1675; Pub. L. 104–106, div. A, title XV, §1502(c)(4)(B), Feb. 10, 1996, 110 Stat. 507; Pub. L. 106–65, div. A, title X, §1067(10), Oct. 5, 1999, 113 Stat. 774; Pub. L. 111–259, title VIII, §805(a)–(d)(1), Oct. 7, 2010, 124 Stat. 2748.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 404b of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2010—Pub. L. 111–259, §805(d)(1), struck out “foreign” after “national” in section catchline.

Subsec. (a). Pub. L. 111–259, §805(a), (b)(1), struck out “foreign” after “national” wherever appearing in heading and text and substituted “Director of National Intelligence” for “Director of Central Intelligence” in text.

Subsec. (b). Pub. L. 111–259, §805(b)(2), inserted “of National Intelligence” after “Director”.

Subsec. (c). Pub. L. 111–259, §805(b)(1), (c), substituted “Director of National Intelligence” for “Director of Central Intelligence” and “future-years defense program submitted pursuant to section 221 of title 10” for “multiyear defense program submitted pursuant to section 114a of title 10”.

1999—Subsec. (d)(2). Pub. L. 106–65 substituted “Committee on Armed Services” for “Committee on National Security”.

1996—Subsec. (a). Pub. L. 104–106, §1502(c)(4)(B)(i), substituted “the congressional committees specified in subsection (d) each year” for “the Committees on Armed Services and Appropriations of the Senate and the House of Representatives and the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives each year”.

Subsec. (d). Pub. L. 104–106, §1502(c)(4)(B)(ii), added subsec. (d).

Statutory Notes and Related Subsidiaries

SHORT TITLE OF 2023 AMENDMENT

Pub. L. 118–31, div. G, title VI, §7601, Dec. 22, 2023, 137 Stat. 1096, provided that: “This title [enacting sections 3344a and 3350a of this title, amending section 3355a of this title, and enacting provisions set out as a note under section 3501 of Title 44, Public Printing and Documents] may be cited as the ‘Sensible Classification Act of 2023’.”

SHORT TITLE OF 2002 AMENDMENT

Pub. L. 107–306, title IX, §901(a), Nov. 27, 2002, 116 Stat. 2432, provided that: “This title [see Tables for classification] may be cited as the ‘Counterintelligence Enhancement Act of 2002’.”

SHORT TITLE OF 2000 AMENDMENT

Pub. L. 106–567, title VII, §701, Dec. 27, 2000, 114 Stat. 2856, provided that: “This title [enacting subchapter III-A of this chapter] may be cited as the ‘Public Interest Declassification Act of 2000’.”

§ 3302. Identification of constituent components of base intelligence budget

The Director of Central Intelligence shall include the same level of budgetary detail for the Base Budget that is provided for Ongoing Initiatives and New Initiatives to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate in the congressional

justification materials for the annual submission of the National Foreign Intelligence Program of each fiscal year.

(Pub. L. 103-359, title VI, § 603, Oct. 14, 1994, 108 Stat. 3433.)

Editorial Notes

CODIFICATION

Section was formerly classified as a note under section 403-1 of this title prior to editorial reclassification as this section.

Statutory Notes and Related Subsidiaries

TRANSFER OF FUNCTIONS

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 3001 of this title.

§ 3303. Construction of intelligence community facilities; Presidential authorization

(a) No project for the construction of any facility, or improvement to any facility, having an estimated Federal cost in excess of \$300,000, may be undertaken in any fiscal year unless specifically identified as a separate item in the President's annual fiscal year budget request or otherwise specifically authorized and appropriated if such facility or improvement would be used primarily by personnel of the intelligence community.

(b) As used in this section, the term "intelligence community" has the same meaning given that term in section 3003(4) of this title.

(Pub. L. 103-335, title VIII, § 8131, Sept. 30, 1994, 108 Stat. 2653.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403-2a of this title prior to editorial reclassification and renumbering as this section.

§ 3304. Limitation on construction of facilities to be used primarily by intelligence community

(a) In general

(1) In general

Except as provided in subsection (b), no project for the construction of any facility to be used primarily by personnel of any component of the intelligence community which has an estimated Federal cost in excess of \$9,000,000 may be undertaken in any fiscal year unless such project is specifically identified as a separate item in the President's annual fiscal year budget request and is specifically authorized by the Congress.

(2) Notification

In the case of a project for the construction of any facility to be used primarily by per-

sonnel of any component of the intelligence community which has an estimated Federal cost greater than \$4,000,000 but less than \$9,000,000, or where any project for the improvement, repair, or modification of such a facility has an estimated Federal cost greater than \$4,000,000, the head of such component, in coordination with and subject to the approval of the Director of National Intelligence, shall submit a notification to the intelligence committees specifically identifying such project.

(b) Exception

(1) In general

Notwithstanding subsection (a) but subject to paragraphs (2) and (3), a project for the construction of a facility to be used primarily by personnel of any component of the intelligence community may be carried out if the Secretary of Defense and the Director of National Intelligence jointly determine—

(A) that the project is vital to the national security or to the protection of health, safety, or the quality of the environment; and

(B) that the requirement for the project is so urgent that deferral of the project for inclusion in the next Act authorizing appropriations for the intelligence community would be inconsistent with national security or the protection of health, safety, or environmental quality, as the case may be.

(2) Report

(A) When a decision is made to carry out a construction project under this subsection, the Secretary of Defense and the Director of National Intelligence jointly shall submit a report in writing to the appropriate committees of Congress on that decision. Each such report shall include (i) the justification for the project and the current estimate of the cost of the project, (ii) the justification for carrying out the project under this subsection, and (iii) a statement of the source of the funds to be used to carry out the project. The project may then be carried out only after the end of the 7-day period beginning on the date the notification is received by such committees.

(B) Notwithstanding subparagraph (A), a project referred to in paragraph (1) may begin on the date the notification is received by the appropriate committees of Congress under that paragraph if the Director of National Intelligence and the Secretary of Defense jointly determine that—

(i) an emergency exists with respect to the national security or the protection of health, safety, or environmental quality; and

(ii) any delay in the commencement of the project would harm any or all of those interests.

(3) Projects primarily for CIA

If a project referred to in paragraph (1) is primarily for the Central Intelligence Agency, the Director of the Central Intelligence Agency shall make the determination and submit the report required by paragraphs (1) and (2).

(4) Limitation

A project carried out under this subsection shall be carried out within the total amount of

funds appropriated for intelligence and intelligence-related activities that have not been obligated.

(c) Application

This section shall not apply to any project which is subject to subsection (a)(1)(A) or (c) of section 601.

(Pub. L. 103-359, title VI, § 602, Oct. 14, 1994, 108 Stat. 3432; Pub. L. 108-177, title III, § 314, Dec. 13, 2003, 117 Stat. 2610; Pub. L. 111-259, title VIII, § 809, Oct. 7, 2010, 124 Stat. 2749; Pub. L. 115-31, div. N, title III, § 307, May 5, 2017, 131 Stat. 813; Pub. L. 116-260, div. W, title III, § 309, Dec. 27, 2020, 134 Stat. 2369; Pub. L. 117-103, div. X, title III, § 305, Mar. 15, 2022, 136 Stat. 966; Pub. L. 118-159, div. F, title LXIX, § 6902(d), Dec. 23, 2024, 138 Stat. 2517.)

Editorial Notes

REFERENCES IN TEXT

Section 601, referred to in subsec. (c), means section 601 of Pub. L. 103-359, title VI, Oct. 14, 1994, 108 Stat. 3431, which is not classified to the Code.

CODIFICATION

Section was formerly classified to section 403-2b of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2024—Subsec. (a)(1). Pub. L. 118-159, § 6902(d)(1), substituted “\$9,000,000” for “\$6,000,000”.

Subsec. (a)(2). Pub. L. 118-159, § 6902(d)(2), substituted “\$4,000,000” for “\$2,000,000” in two places and “\$9,000,000” for “\$6,000,000”.

2022—Subsec. (a). Pub. L. 117-103 substituted “\$6,000,000” for “\$5,000,000” in pars. (1) and (2).

2020—Subsec. (a)(2). Pub. L. 116-260 substituted “\$2,000,000” for “\$1,000,000” in two places and substituted “the head of such component, in coordination with and subject to the approval of the Director of National Intelligence, shall submit a notification” for “the Director of National Intelligence shall submit a notification”.

2017—Subsec. (a)(2). Pub. L. 115-31 substituted “project for the improvement, repair, or modification of” for “improvement project to”.

2010—Subsecs. (a)(2), (b)(1), (2)(A), (B). Pub. L. 111-259, § 809(1), (2)(A), (B), substituted “Director of National Intelligence” for “Director of Central Intelligence”.

Subsec. (b)(3). Pub. L. 111-259, § 809(2)(C), substituted “Director of the Central Intelligence Agency” for “Director of Central Intelligence”.

2003—Subsec. (a). Pub. L. 108-177, § 314(a), substituted “\$5,000,000” for “\$750,000” in pars. (1) and (2) and “\$1,000,000” for “\$500,000” in two places in par. (2).

Subsec. (b)(2). Pub. L. 108-177, § 314(b), designated existing provisions as subpar. (A), redesignated former subpars. (A) to (C) as cls. (i) to (iii), respectively, substituted “7-day period” for “21-day period”, and added subpar. (B).

Statutory Notes and Related Subsidiaries

DEFINITIONS

Pub. L. 103-359, title VI, § 604, Oct. 14, 1994, 108 Stat. 3433, provided that: “As used in this title [enacting this section and section 3302 of this title]:

“(1) INTELLIGENCE COMMITTEES.—The term ‘intelligence committees’ means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

“(2) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the same meaning given that

term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4) [now 50 U.S.C. 3003(4)]).”

§ 3305. Exhibits for inclusion with budget justification books

Beginning with the fiscal year 2010 budget request, the Director of National Intelligence shall include the budget exhibits identified in paragraphs (1) and (2) as described in the Department of Defense Financial Management Regulation with the congressional budget justification books.

(1) For procurement programs requesting more than \$20,000,000 in any fiscal year, the P-1, Procurement Program; P-5, Cost Analysis; P-5a, Procurement History and Planning; P-21, Production Schedule; and P-40¹ Budget Item Justification.

(2) For research, development, test and evaluation projects requesting more than \$10,000,000 in any fiscal year, the R-1, RDT&E Program; R-2, RDT&E Budget Item Justification; R-3, RDT&E Project Cost Analysis; and R-4, RDT&E Program Schedule Profile.

(Pub. L. 110-329, div. C, title VIII, § 8107, Sept. 30, 2008, 122 Stat. 3644.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 415a-2 of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries

SIMILAR PROVISIONS

Provisions similar to those in this section were contained in the following appropriation acts:

Pub. L. 113-6, div. C, title VIII, § 8087, Mar. 26, 2013, 127 Stat. 317.

Pub. L. 112-74, div. A, title VIII, § 8090, Dec. 23, 2011, 125 Stat. 827.

Pub. L. 112-10, div. A, title VIII, § 8091, Apr. 15, 2011, 125 Stat. 77.

Pub. L. 111-118, div. A, title VIII, § 8100, Dec. 19, 2009, 123 Stat. 3450.

§ 3306. Availability to public of certain intelligence funding information

(a) Budget request

At the time that the President submits to Congress the budget for a fiscal year pursuant to section 1105 of title 31, the President shall disclose to the public the aggregate amount of appropriations requested for that fiscal year for the National Intelligence Program.

(b) Amounts appropriated each fiscal year

Not later than 30 days after the end of each fiscal year, the Director of National Intelligence shall disclose to the public the aggregate amount of funds appropriated by Congress for the National Intelligence Program for such fiscal year.

(c) Waiver

(1) In general

The President may waive or postpone the disclosure required by subsection (a) or (b) for

¹ So in original. Probably should be followed by a comma.

a fiscal year by submitting to the Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives—

(A) a statement, in unclassified form, that the disclosure required in subsection (a) or (b) for that fiscal year would damage national security; and

(B) a statement detailing the reasons for the waiver or postponement, which may be submitted in classified form.

(2) Submission dates

The President shall submit the statements required under paragraph (1)—

(A) in the case of a waiver or postponement of a disclosure required under subsection (a), at the time of the submission of the budget for the fiscal year for which such disclosure is waived or postponed; and

(B) in the case of a waiver or postponement of a disclosure required under subsection (b), not later than 30 days after the date of the end of the fiscal year for which such disclosure is waived or postponed.

(d) Definition

As used in this section, the term “National Intelligence Program” has the meaning given the term in section 3003(6) of this title.

(Pub. L. 110–53, title VI, §601, Aug. 3, 2007, 121 Stat. 335; Pub. L. 111–259, title III, §364, Oct. 7, 2010, 124 Stat. 2702.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 415c of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2010—Pub. L. 111–259 amended section generally. Prior to amendment, section related to availability to public of certain intelligence funding information.

Statutory Notes and Related Subsidiaries

INCREASED TRANSPARENCY REGARDING COUNTERTERRORISM BUDGET OF THE UNITED STATES

Pub. L. 116–92, div. E, title LVII, §5702, Dec. 20, 2019, 133 Stat. 2160, provided that:

“(a) FINDINGS.—Congress finds the following:

“(1) Consistent with section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a)), the recent practice of the intelligence community has been to release to the public—

“(A) around the date on which the President submits to Congress a budget for a fiscal year pursuant to section 1105 of title 31, United States Code, the ‘top-line’ amount of total funding requested for the National Intelligence Program for such fiscal year; and

“(B) the amount of requested and appropriated funds for the National Intelligence Program and Military Intelligence Program for certain prior fiscal years, consistent with the protection of intelligence sources and methods.

“(2) The Directorate of Strategic Operational Planning of the National Counterterrorism Center is responsible for producing an annual National Counterterrorism Budget report, which examines the alignment of intelligence and other resources in the applicable fiscal year budget with the

counterterrorism goals and areas of focus in the National Strategy for Counterterrorism.

“(b) SENSE OF CONGRESS.—It is the sense of Congress that—

“(1) despite the difficulty of compiling and releasing to the public comprehensive information on the resource commitments of the United States to counterterrorism activities and programs, including with respect to such activities and programs of the intelligence community, the United States Government could take additional steps to enhance the understanding of the public with respect to such resource commitments, in a manner consistent with the protection of intelligence sources and methods and other national security interests; and

“(2) the United States Government should release to the public as much information as possible regarding the funding of counterterrorism activities and programs, including activities and programs of the intelligence community, in a manner consistent with the protection of intelligence sources and methods and other national security interests.

“(c) BRIEFING ON PUBLIC RELEASE OF INFORMATION.—

“(1) REQUIREMENT.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], and not later than 90 days after the beginning of each fiscal year thereafter, the President shall ensure that the congressional intelligence committees receive a briefing from appropriate personnel of the United States Government on the feasibility of releasing to the public additional information relating to counterterrorism efforts of the intelligence community.

“(2) ELEMENTS.—Each briefing required by paragraph (1) shall include a discussion of the feasibility of—

“(A) subject to paragraph (3), releasing to the public the National Counterterrorism Budget report described in subsection (a)(2) for the prior fiscal year; and

“(B) declassifying other reports, documents, or activities of the intelligence community relating to counterterrorism and releasing such information to the public in a manner consistent with the protection of intelligence sources and methods and other national security interests.

“(3) RELEASE OF NATIONAL COUNTERTERRORISM BUDGET REPORT.—The President may satisfy the requirement under paragraph (2)(A) during a fiscal year by, not later than 90 days after the beginning of the fiscal year, releasing to the public the National Counterterrorism Budget report (with any redactions the Director determines necessary to protect intelligence sources and methods and other national security interests) for the prior fiscal year.”

[For definitions of “intelligence community” and “congressional intelligence committees” as used in section 5702 of Pub. L. 116–92, set out above, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.]

§ 3307. Communications with the Committees on Armed Services of the Senate and the House of Representatives

(a) Requests of committees

The Director of the National Counterterrorism Center, the Director of a national intelligence center, or the head of any element of the intelligence community shall, not later than 45 days after receiving a written request from the Chair or ranking minority member of the Committee on Armed Services of the Senate or the Committee on Armed Services of the House of Representatives for any existing intelligence assessment, report, estimate, or legal opinion relating to matters within the jurisdiction of such Committee, make available to such committee such

assessment, report, estimate, or legal opinion, as the case may be.

(b) Assertion of privilege

(1) In general

In response to a request covered by subsection (a), the Director of the National Counterterrorism Center, the Director of a national intelligence center, or the head of any element of the intelligence community shall provide to the Committee making such request the document or information covered by such request unless the President determines that such document or information shall not be provided because the President is asserting a privilege pursuant to the Constitution of the United States.

(2) Submission to Congress

The White House Counsel shall submit to Congress in writing any assertion by the President under paragraph (1) of a privilege pursuant to the Constitution.

(c) Definitions

In this section:

(1) Intelligence community

The term “intelligence community” has the meaning given the term in section 3003(4) of this title.

(2) Intelligence assessment

The term “intelligence assessment” means an intelligence-related analytical study of a subject of policy significance and does not include building-block papers, research projects, and reference aids.

(3) Intelligence estimate

The term “intelligence estimate” means an appraisal of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to an enemy or potential enemy and the probable order of adoption of such courses of action.

(Pub. L. 110–181, div. A, title X, §1079, Jan. 28, 2008, 122 Stat. 334.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 413c of this title prior to editorial reclassification and renumbering as this section.

§ 3308. Information access by the Comptroller General of the United States

(a) DNI directive governing access

(1) Requirement for directive

The Director of National Intelligence, in consultation with the Comptroller General of the United States, shall issue a written directive governing the access of the Comptroller General to information in the possession of an element of the intelligence community.

(2) Amendment to directive

The Director of National Intelligence, in consultation with the Comptroller General, may issue an amendment to the directive issued under paragraph (1) at any time the Di-

rector determines such an amendment is appropriate.

(3) Relationship to other laws

The directive issued under paragraph (1) and any amendment to such directive issued under paragraph (2) shall be consistent with the provisions of—

(A) chapter 7 of title 31; and

(B) the National Security Act of 1947 (50 U.S.C. 401 et seq.).

(b) Confidentiality of information

(1) Requirement for confidentiality

The Comptroller General of the United States shall ensure that the level of confidentiality of information made available to the Comptroller General pursuant to the directive issued under subsection (a)(1) or an amendment to such directive issued under subsection (a)(2) is not less than the level of confidentiality of such information required of the head of the element of the intelligence community from which such information was obtained.

(2) Penalties for unauthorized disclosure

An officer or employee of the Government Accountability Office shall be subject to the same statutory penalties for unauthorized disclosure or use of such information as an officer or employee of the element of the intelligence community from which such information was obtained.

(c) Submission to Congress

(1) Submission of directive

The directive issued under subsection (a)(1) shall be submitted to Congress by the Director of National Intelligence, together with any comments of the Comptroller General of the United States, no later than May 1, 2011.

(2) Submission of amendment

Any amendment to such directive issued under subsection (a)(2) shall be submitted to Congress by the Director, together with any comments of the Comptroller General.

(d) Effective date

The directive issued under subsection (a)(1) and any amendment to such directive issued under subsection (a)(2) shall take effect 60 days after the date such directive or amendment is submitted to Congress under subsection (c), unless the Director determines that for reasons of national security the directive or amendment should take effect sooner.

(Pub. L. 111–259, title III, §348, Oct. 7, 2010, 124 Stat. 2700.)

Editorial Notes

REFERENCES IN TEXT

The National Security Act of 1947, referred to in subsec. (a)(3)(B), is act July 26, 1947, ch. 343, 61 Stat. 495, which is classified principally to chapter 44 (§3001 et seq.) of this title. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was formerly classified to section 403–9 of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries**DEFINITION**

For definition of “intelligence community”, see section 2 of Pub. L. 111-259, set out as a note under section 3003 of this title.

§ 3308a. Provision of certain information to Government Accountability Office by National Reconnaissance Office

(a) In general

The Director of the National Reconnaissance Office shall provide to the Comptroller General of the United States, in a timely manner, access to the cost, schedule, and performance information the Comptroller General requires to conduct assessments, as required by any of the appropriate congressional committees, of programs of the National Reconnaissance Office.

(b) Appropriate congressional committees defined

In this section, the term “appropriate congressional committees” means—

- (1) the congressional defense committees; and
- (2) the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(Pub. L. 114-328, div. A, title XVI, §1620, Dec. 23, 2016, 130 Stat. 2596.)

Statutory Notes and Related Subsidiaries**“CONGRESSIONAL DEFENSE COMMITTEES” DEFINED**

Congressional defense committees means the Committees on Armed Services and Appropriations of the Senate and the House of Representatives, see section 3 of Pub. L. 114-328, 130 Stat. 2025. See note under section 101 of Title 10, Armed Forces.

§ 3309. Notification of establishment of advisory committee

The Director of National Intelligence and the Director of the Central Intelligence Agency shall each notify the congressional intelligence committees each time each such Director creates an advisory committee. Each notification shall include—

- (1) a description of such advisory committee, including the subject matter of such committee; and
- (2) a list of members of such advisory committee; and
- (3) in the case of an advisory committee created by the Director of National Intelligence, the reasons for a determination by the Director under section 1003(b)(3) of title 5 that an advisory committee cannot comply with the requirements of chapter 10 of title 5.

(Pub. L. 111-259, title IV, §410(b), Oct. 7, 2010, 124 Stat. 2725; Pub. L. 113-126, title III, §329(b)(1), July 7, 2014, 128 Stat. 1406; Pub. L. 117-286, §4(a)(319), Dec. 27, 2022, 136 Stat. 4341.)

Editorial Notes**CODIFICATION**

Section was formerly classified as a note under section 405 of this title prior to editorial reclassification as this section.

AMENDMENTS

2022—Par. (3). Pub. L. 117-286 substituted “section 1003(b)(3) of title 5 that an advisory committee cannot comply with the requirements of chapter 10 of title 5.” for “section 4(b)(3) of the Federal Advisory Committee Act (5 U.S.C. App.) that an advisory committee cannot comply with the requirements of such Act.”

2014—Pub. L. 113-126 amended section generally. Prior to amendment, section related to annual report on advisory committees created by Director of National Intelligence and Director of the Central Intelligence Agency, contents of report, and inclusion of reasons for ODNI exclusion of advisory committee from Federal Advisory Committee Act.

Statutory Notes and Related Subsidiaries**DEFINITION**

For definition of “congressional intelligence committees” as used in this section, see section 2 of Pub. L. 111-259, set out as a note under section 3003 of this title.

§ 3310. Annual report on United States security arrangements and commitments with other nations

(a) Report requirements

The President shall submit to the congressional committees specified in subsection (d) each year a report (in both classified and unclassified form) on United States security arrangements with, and commitments to, other nations.

(b) Matters to be included

The President shall include in each such report the following:

(1) A description of—

- (A) each security arrangement with, or commitment to, other nations, whether based upon (i) a formal document (including a mutual defense treaty, a pre-positioning arrangement or agreement, or an access agreement), or (ii) an expressed policy; and
- (B) the historical origins of each such arrangement or commitment.

(2) An evaluation of the ability of the United States to meet its commitments based on the projected reductions in the defense structure of the United States.

(3) A plan for meeting each of those commitments with the force structure projected for the future.

(4) An assessment of the need to continue, modify, or discontinue each of those arrangements and commitments in view of the changing international security situation.

(c) Deadline for report

The President shall submit the report required by subsection (a) not later than February 1 of each year.

(d) Specified congressional committees

The congressional committees referred to in subsection (a) are the following:

- (1) The Committee on Armed Services and the Committee on Foreign Relations of the Senate.
- (2) The Committee on Armed Services and the Committee on International Relations of the House of Representatives.

(Pub. L. 101-510, div. A, title XIV, §1457, Nov. 5, 1990, 104 Stat. 1696; Pub. L. 104-106, div. A, title

XV, § 1502(c)(4)(C), Feb. 10, 1996, 110 Stat. 507; Pub. L. 106-65, div. A, title X, § 1067(10), Oct. 5, 1999, 113 Stat. 774.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 404c of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

1999—Subsec. (d)(2). Pub. L. 106-65 substituted “Committee on Armed Services” for “Committee on National Security”.

1996—Subsec. (a). Pub. L. 104-106, § 1502(c)(4)(C)(i), substituted “shall submit to the congressional committees specified in subsection (d) each year” for “shall submit to the Committees on Armed Services and on Foreign Affairs of the House of Representatives and the Committees on Armed Services and Foreign Relations of the Senate each year”.

Subsec. (c). Pub. L. 104-106, § 1502(c)(4)(C)(ii), substituted “The President” for “(1) Except as provided in paragraph (2), the President” and struck out par. (2) which read as follows: “In the case of the report required to be submitted in 1991, the evaluation, plan, and assessment referred to in paragraphs (2), (3), and (4) of subsection (b) may be submitted not later than May 1, 1991.”

Subsec. (d). Pub. L. 104-106, § 1502(c)(4)(C)(iii), added subsec. (d).

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on International Relations of House of Representatives changed to Committee on Foreign Affairs of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

§ 3311. Submittal to Congress by heads of elements of intelligence community of plans for orderly shutdown in event of absence of appropriations

(a) In general

Whenever the head of an applicable agency submits a plan to the Director of the Office of Management and Budget in accordance with section 124 of Office of Management and Budget Circular A-11, pertaining to agency operations in the absence of appropriations, or any successor circular of the Office that requires the head of an applicable agency to submit to the Director a plan for an orderly shutdown in the event of the absence of appropriations, such head shall submit a copy of such plan to the following:

- (1) The congressional intelligence committees.
- (2) The Subcommittee on Defense of the Committee on Appropriations of the Senate.
- (3) The Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

(4) In the case of a plan for an element of the intelligence community that is within the Department of Defense, to—

- (A) the Committee on Armed Services of the Senate; and
- (B) the Committee on Armed Services of the House of Representatives.

(b) Head of an applicable agency defined

In this section, the term “head of an applicable agency” includes the following:

- (1) The Director of National Intelligence.
- (2) The Director of the Central Intelligence Agency.
- (3) Each head of each element of the intelligence community that is within the Department of Defense.

(Pub. L. 113-126, title III, § 323, July 7, 2014, 128 Stat. 1401.)

Statutory Notes and Related Subsidiaries

DEFINITION

For definition of “congressional intelligence committees” as used in this section, see section 2 of Pub. L. 113-126, set out as a note under section 3003 of this title.

§ 3312. Repealed. Pub. L. 117-263, div. F, title LXIII, § 6316(c), Dec. 23, 2022, 136 Stat. 3513

Section, Pub. L. 115-31, div. N, title III, § 310, May 5, 2017, 131 Stat. 815, provided for congressional oversight of policy directives and guidance.

§ 3313. Notification of memoranda of understanding

(a) In general

Each year, concurrent with the annual budget request submitted by the President to Congress under section 1105 of title 31, each head of an element of the intelligence community shall submit to the congressional intelligence committees a report that lists each memorandum of understanding or other agreement regarding significant operational activities or policy entered into during the most recently completed fiscal year between or among such element and any other entity of the United States Government.

(b) Provision of documents

Each head of an element of an intelligence community who receives a request from the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives for a copy of a memorandum of understanding or other document listed in a report submitted by the head under subsection (a) shall submit to such committee the requested copy as soon as practicable after receiving such request.

(c) Administrative memorandum or agreement

Nothing in this section may be construed to require an element of the intelligence community to submit to the congressional intelligence committees any memorandum or agreement that is solely administrative in nature, including a memorandum or agreement regarding joint duty or other routine personnel assignments.

(Pub. L. 115-31, div. N, title III, § 311, May 5, 2017, 131 Stat. 815; Pub. L. 116-92, div. E, title LXVII, § 6723, Dec. 20, 2019, 133 Stat. 2234.)

Editorial Notes

AMENDMENTS

2019—Pub. L. 116-92 added subsecs. (a) and (b), redesignated former subsec. (b) as (c) and struck out former subsec. (a). Text read as follows: “The head of each element of the intelligence community shall submit to the congressional intelligence committees a copy of each memorandum of understanding or other agree-

ment regarding significant operational activities or policy between or among such element and any other entity or entities of the United States Government—

“(1) for such a memorandum or agreement that is in effect on May 5, 2017, not later than 60 days after such date; and

“(2) for such a memorandum or agreement entered into after such date, in a timely manner and not more than 60 days after the date such memorandum or other agreement is entered into.”

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 2 of div. N of Pub. L. 115-31, set out as a note under section 3003 of this title.

§ 3314. Report on national security systems

(a) Appropriate committees of Congress defined

In this section, the term “appropriate committees of Congress” means—

- (1) the congressional intelligence committees;
- (2) the Committee on Appropriations and the Committee on Armed Services of the Senate; and
- (3) the Committee on Appropriations and the Committee on Armed Services of the House of Representatives.

(b) Report

Not later than 120 days after May 5, 2017, and annually thereafter, the Director of the National Security Agency, in coordination with the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, shall submit to the appropriate committees of Congress a report on national security systems.

(c) Content

Each report submitted under subsection (b) shall include information related to—

- (1) national security systems or components thereof that have been decertified and are still in operational use;
- (2) extension requests and the current status of any national security systems still in use or components thereof that have been decertified and are still in use;
- (3) national security systems known to not be in compliance with the policies, principles, standards, and guidelines issued by the Committee on National Security Systems established pursuant to National Security Directive 42, signed by the President on July 5, 1990; and
- (4) organizations which have not provided access or information to the Director of the National Security Agency that is adequate to enable the Director to make a determination as to whether such organizations are in compliance with the policies, principles, standards, and guidelines issued by such Committee on National Security Systems.

(Pub. L. 115-31, div. N, title VI, § 603, May 5, 2017, 131 Stat. 829.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 2 of div. N of

Pub. L. 115-31, set out as a note under section 3003 of this title.

§ 3315. Repealed. Pub. L. 117-103, div. X, title V, § 504(e), Mar. 15, 2022, 136 Stat. 988

Section, Pub. L. 115-31, div. N, title VI, § 608(b), May 5, 2017, 131 Stat. 833, required annual certification of controlled access programs to the congressional intelligence committees.

§ 3316. Submission of intelligence community policies

(a) Definitions

In this section:

(1) Electronic repository

The term “electronic repository” means the electronic distribution mechanism, in use as of December 20, 2019, or any successor electronic distribution mechanism, by which the Director of National Intelligence submits to the congressional intelligence committees information.

(2) Policy

The term “policy”, with respect to the intelligence community, includes unclassified or classified—

- (A) directives, policy guidance, and policy memoranda of the intelligence community;
- (B) executive correspondence of the Director of National Intelligence; and
- (C) any equivalent successor policy instruments.

(b) Submission of policies

(1) Current policy

Not later than 180 days after December 20, 2019, the Director of National Intelligence shall submit to the congressional intelligence committees using the electronic repository all nonpublicly available policies issued by the Director of National Intelligence for the intelligence community that are in effect as of the date of the submission.

(2) Continuous updates

Not later than 15 days after the date on which the Director of National Intelligence issues, modifies, or rescinds a policy of the intelligence community, the Director shall—

- (A) notify the congressional intelligence committees of such addition, modification, or removal; and
- (B) update the electronic repository with respect to such addition, modification, or removal.

(Pub. L. 116-92, div. E, title LXIII, § 6315, Dec. 20, 2019, 133 Stat. 2194.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3316a. Reports on intelligence community participation in vulnerabilities equities process of Federal Government

(a) Definitions

In this section:

(1) Vulnerabilities Equities Policy and Process document

The term “Vulnerabilities Equities Policy and Process document” means the executive branch document entitled “Vulnerabilities Equities Policy and Process” dated November 15, 2017.

(2) Vulnerabilities Equities Process

The term “Vulnerabilities Equities Process” means the interagency review of vulnerabilities, pursuant to the Vulnerabilities Equities Policy and Process document or any successor document.

(3) Vulnerability

The term “vulnerability” means a weakness in an information system or its components (for example, system security procedures, hardware design, and internal controls) that could be exploited or could affect confidentiality, integrity, or availability of information.

(b) Reports on process and criteria under Vulnerabilities Equities Policy and Process

(1) In general

Not later than 90 days after December 20, 2019, the Director of National Intelligence shall submit to the congressional intelligence committees a written report describing—

(A) with respect to each element of the intelligence community—

(i) the title of the official or officials responsible for determining whether, pursuant to criteria contained in the Vulnerabilities Equities Policy and Process document or any successor document, a vulnerability must be submitted for review under the Vulnerabilities Equities Process; and

(ii) the process used by such element to make such determination; and

(B) the roles or responsibilities of that element during a review of a vulnerability submitted to the Vulnerabilities Equities Process.

(2) Changes to process or criteria

Not later than 30 days after any significant change is made to the process and criteria used by any element of the intelligence community for determining whether to submit a vulnerability for review under the Vulnerabilities Equities Process, such element shall submit to the congressional intelligence committees a report describing such change.

(3) Form of reports

Each report submitted under this subsection shall be submitted in unclassified form, but may include a classified annex.

(c) Annual reports

(1) In general

Not less frequently than once each calendar year, the Director of National Intelligence shall submit to the congressional intelligence committees a classified report containing, with respect to the previous year—

(A) the number of vulnerabilities submitted for review under the Vulnerabilities Equities Process;

(B) the number of vulnerabilities described in subparagraph (A) disclosed to each vendor responsible for correcting the vulnerability, or to the public, pursuant to the Vulnerabilities Equities Process; and

(C) the aggregate number, by category, of the vulnerabilities excluded from review under the Vulnerabilities Equities Process, as described in paragraph 5.4 of the Vulnerabilities Equities Policy and Process document.

(2) Unclassified information

Each report submitted under paragraph (1) shall include an unclassified appendix that contains—

(A) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process; and

(B) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process known to have been patched.

(3) Nonduplication

The Director of National Intelligence may forgo submission of an annual report required under this subsection for a calendar year, if the Director notifies the intelligence committees in writing that, with respect to the same calendar year, an annual report required by paragraph 4.3 of the Vulnerabilities Equities Policy and Process document already has been submitted to Congress, and such annual report contains the information that would otherwise be required to be included in an annual report under this subsection.

(4) Publication

The Director of National Intelligence shall make available to the public each unclassified appendix submitted with a report under paragraph (1) pursuant to paragraph (2).

(Pub. L. 116–92, div. E, title LXVII, § 6720, Dec. 20, 2019, 133 Stat. 2230; Pub. L. 117–103, div. X, title III, § 307, Mar. 15, 2022, 136 Stat. 966.)

Editorial Notes

AMENDMENTS

2022—Subsec. (c)(4). Pub. L. 117–103 added par. (4).

Statutory Notes and Related Subsidiaries

DEFINITIONS

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

§ 3316b. Continuity of operations plans for certain elements of the intelligence community in the case of a national emergency

(a) Definition of covered national emergency

In this section, the term “covered national emergency” means the following:

(1) A major disaster declared by the President under section 5170 of title 42.

(2) An emergency declared by the President under section 5191 of title 42.

(3) A national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.).

(4) A public health emergency declared under section 247d of title 42.

(b) In general

The Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Reconnaissance Office, the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency shall each establish continuity of operations plans for use in the case of covered national emergencies for the element of the intelligence community concerned.

(c) Submission to Congress

(1) Director of National Intelligence and Director of the Central Intelligence Agency

Not later than 7 days after the date on which a covered national emergency is declared, the Director of National Intelligence and the Director of the Central Intelligence Agency shall each submit to the congressional intelligence committees the plan established under subsection (b) for that emergency for the element of the intelligence community concerned.

(2) Director of National Reconnaissance Office, Director of Defense Intelligence Agency, Director of National Security Agency, and Director of National Geospatial-Intelligence Agency

Not later than 7 days after the date on which a covered national emergency is declared, the Director of the National Reconnaissance Office, the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency shall each submit the plan established under subsection (b) for that emergency for the element of the intelligence community concerned to the following:

- (A) The congressional intelligence committees.
- (B) The Committee on Armed Services of the Senate.
- (C) The Committee on Armed Services of the House of Representatives.

(d) Updates

During a covered national emergency, the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Reconnaissance Office, the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency shall each submit any updates to the plans submitted under subsection (c)—

- (1) in accordance with that subsection; and
- (2) in a timely manner consistent with section 3091 of this title.

(Pub. L. 116–260, div. W, title III, § 303, Dec. 27, 2020, 134 Stat. 2364.)

Editorial Notes

REFERENCES IN TEXT

The National Emergencies Act, referred to in subsec. (a)(3), is Pub. L. 94–412, Sept. 14, 1976, 90 Stat. 1255,

which is classified principally to chapter 34 (§1601 et seq.) of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of this title and Tables.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “congressional intelligence committees” and “intelligence community” as used in this section, see section 2 of div. W of Pub. L. 116–260, set out as a note under section 3003 of this title.

§ 3316c. Development of definitions for certain terms relating to intelligence

(a) Development

Not later than September 30, 2023, the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security, in consultation with the heads of the elements of the intelligence community, shall jointly develop and publish definitions for the following terms:

- (1) Acoustic intelligence.
- (2) All-source intelligence.
- (3) Communications intelligence.
- (4) Critical intelligence.
- (5) Cyber-threat intelligence.
- (6) Electronic intelligence.
- (7) Explosive ordnance intelligence.
- (8) General military intelligence.
- (9) Imagery intelligence.
- (10) Geospatial intelligence.
- (11) Instrumentation signals intelligence.
- (12) Intelligence-related activity.
- (13) Joint intelligence.
- (14) Measurement and signature intelligence.
- (15) Medical intelligence.
- (16) Open-source intelligence.
- (17) Operational intelligence.
- (18) Scientific and technical intelligence.
- (19) Signals intelligence.
- (20) Strategic intelligence.
- (21) Tactical intelligence.
- (22) Target intelligence.
- (23) Technical intelligence.
- (24) Such others terms as may be jointly determined necessary by the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security.

(b) Application to activities of intelligence community

The Director of National Intelligence shall ensure that the definitions developed under subsection (a) are used uniformly across activities of the intelligence community with respect to the corresponding terms specified in such subsection.

(c) Notice of modifications

The Director of National Intelligence and the Under Secretary of Defense for Intelligence shall submit to the appropriate congressional committees notification of any modification by the Director and Under Secretary to a definition of a term specified in subsection (a) following the initial publication of the definition under such subsection.

(d) Appropriate congressional committees defined

In this section, the term “appropriate congressional committees” means—

(1) the congressional intelligence committees; and

(2) the Committees on Armed Services of the House of Representatives and the Senate.

(Pub. L. 117–103, div. X, title III, § 309, Mar. 15, 2022, 136 Stat. 971.)

Statutory Notes and Related Subsidiaries

REQUIREMENT TO DEVELOP LEXICON FOR TERMS RELATING TO GRAY ZONE ACTIVITIES

Pub. L. 117–103, div. X, title VIII, § 825(b)(5), (c), Mar. 15, 2022, 136 Stat. 1028, 1029, provided that:

[(“b) NATIONAL INTELLIGENCE ESTIMATE.—]

“(5) DEFINITIONS.—In this subsection [pars. (1) to (4) not classified to the Code]:

“(A) GRAY ZONE ACTIVITY.—The term ‘gray zone activity’ means an activity to advance the national interests of a State that—

“(i) falls between ordinary statecraft and open warfare;

“(ii) is carried out with an intent to maximize the advancement of interests of the state without provoking a kinetic military response by the United States; and

“(iii) falls on a spectrum that ranges from covert adversary operations, to detectible covert adversary operations, to unattributable adversary operations, to deniable adversary operations, to open adversary operations.

“(B) COVERT ADVERSARY OPERATION.—The term ‘covert adversary operation’ means an operation by an adversary that—

“(i) the adversary intends to remain below the threshold at which the United States detects the operation; and

“(ii) does stay below such threshold.

“(C) DETECTIBLE COVERT ADVERSARY OPERATION.—The term ‘detectible covert adversary operation’ means an operation by an adversary that—

“(i) the adversary intends to remain below the threshold at which the United States detects the operation; but

“(ii) is ultimately detected by the United States at a level below the level at which the United States will publicly attribute the operation to the adversary.

“(D) UNATTRIBUTABLE ADVERSARY OPERATION.—The term ‘unattributable adversary operation’ means an operation by an adversary that the adversary intends to be detected by the United States, but remains below the threshold at which the United States will publicly attribute the operation to the adversary.

“(E) DENIABLE ADVERSARY OPERATION.—The term ‘deniable adversary operation’ means an operation by an adversary that—

“(i) the adversary intends to be detected and publicly or privately attributed by the United States; and

“(ii) the adversary intends to deny, to limit the response by the United States, and any allies of the United States.

“(F) OPEN ADVERSARY OPERATION.—The term ‘open adversary operation’ means an operation by an adversary that the adversary openly acknowledges as attributable to the adversary.

“(c) REQUIREMENT TO DEVELOP LEXICON.—

“(1) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall develop a lexicon of common terms (and corresponding definitions for such terms) for concepts associated with gray zone activities.

“(2) CONSIDERATIONS.—In developing the lexicon under paragraph (1), the National Intelligence Council shall include in the lexicon each term (and the corresponding definition for each term) specified in subsection (b)(5), unless the National Intelligence

Council determines that an alternative term (or alternative definition)—

“(A) more accurately describes a concept associated with gray zone activities; or

“(B) is preferable for any other reason.

“(3) REPORT.—

“(A) PUBLICATION.—The Director of National Intelligence shall publish a report containing the lexicon developed under paragraph (1).

“(B) FORM.—The report under subparagraph (A) shall be published in unclassified form.”

DEFINITIONS

For definitions of “congressional intelligence committees” and “intelligence community” as used in this section, see section 2 of div. X of Pub. L. 117–103, set out as a note under section 3003 of this title.

SUBCHAPTER II—PERSONNEL AND ADMINISTRATIVE AUTHORITIES

§ 3321. National Intelligence Reserve Corps

(a) Establishment

The Director of National Intelligence may provide for the establishment and training of a National Intelligence Reserve Corps (in this section referred to as “National Intelligence Reserve Corps”) for the temporary reemployment on a voluntary basis of former employees of elements of the intelligence community during periods of emergency, as determined by the Director.

(b) Eligible individuals

An individual may participate in the National Intelligence Reserve Corps only if the individual previously served as a full time employee of an element of the intelligence community.

(c) Terms of participation

The Director of National Intelligence shall prescribe the terms and conditions under which eligible individuals may participate in the National Intelligence Reserve Corps.

(d) Expenses

The Director of National Intelligence may provide members of the National Intelligence Reserve Corps transportation and per diem in lieu of subsistence for purposes of participating in any training that relates to service as a member of the Reserve Corps.

(e) Treatment of annuitants

(1) If an annuitant receiving an annuity from the Civil Service Retirement and Disability Fund becomes temporarily reemployed pursuant to this section, such annuity shall not be discontinued thereby.

(2) An annuitant so reemployed shall not be considered an employee for the purposes of chapter 83 or 84 of title 5.

(f) Treatment under Office of Director of National Intelligence personnel ceiling

A member of the National Intelligence Reserve Corps who is reemployed on a temporary basis pursuant to this section shall not count against any personnel ceiling applicable to the Office of the Director of National Intelligence.

(Pub. L. 108–458, title I, § 1053, Dec. 17, 2004, 118 Stat. 3683.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403-1c of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

For Determination by President that section take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

§ 3322. Additional education and training requirements**(a) Findings**

Congress makes the following findings:

(1) Foreign language education is essential for the development of a highly-skilled workforce for the intelligence community.

(2) Since September 11, 2001, the need for language proficiency levels to meet required national security functions has been raised, and the ability to comprehend and articulate technical and scientific information in foreign languages has become critical.

(b) Linguistic requirements

(1) The Director of National Intelligence shall—

(A) identify the linguistic requirements for the Office of the Director of National Intelligence;

(B) identify specific requirements for the range of linguistic skills necessary for the intelligence community, including proficiency in scientific and technical vocabularies of critical foreign languages; and

(C) develop a comprehensive plan for the Office to meet such requirements through the education, recruitment, and training of linguists.

(2) In carrying out activities under paragraph (1), the Director shall take into account education grant programs of the Department of Defense and the Department of Education that are in existence as of December 17, 2004.

(c) Professional intelligence training

The Director of National Intelligence shall require the head of each element and component within the Office of the Director of National Intelligence who has responsibility for professional intelligence training to periodically review and revise the curriculum for the professional intelligence training of the senior and intermediate level personnel of such element or component in order to—

(1) strengthen the focus of such curriculum on the integration of intelligence collection and analysis throughout the Office; and

(2) prepare such personnel for duty with other departments, agencies, and elements of the intelligence community.

(Pub. L. 108-458, title I, §1041, Dec. 17, 2004, 118 Stat. 3678; Pub. L. 112-87, title III, §311(a), Jan. 3, 2012, 125 Stat. 1886.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403-1b of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2012—Subsec. (b)(3), (4). Pub. L. 112-87 struck out pars. (3) and (4) which read as follows:

“(3) Not later than one year after December 17, 2004, and annually thereafter, the Director shall submit to Congress a report on the requirements identified under paragraph (1), including the success of the Office of the Director of National Intelligence in meeting such requirements. Each report shall notify Congress of any additional resources determined by the Director to be required to meet such requirements.

“(4) Each report under paragraph (3) shall be in unclassified form, but may include a classified annex.”

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

For Determination by President that section take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

PILOT PROJECT ON CIVILIAN LINGUIST RESERVE CORPS

Pub. L. 109-364, div. A, title IX, §944(a)(1), Oct. 17, 2006, 120 Stat. 2366, transferred administration of pilot project on establishment of Civilian Linguist Reserve Corps required by section 613 of the Intelligence Authorization Act for Fiscal Year 2005 [Pub. L. 108-487, formerly set out as a note below] from Director of National Intelligence to Secretary of Defense.

Pub. L. 109-163, div. A, title XI, §1124, Jan. 6, 2006, 119 Stat. 3454, authorized Secretary of Defense to support implementation of Civilian Linguist Reserve Corps pilot project authorized by section 613 of the Intelligence Authorization Act for Fiscal Year 2005 [Pub. L. 108-487, formerly set out as a note below], subject to availability of appropriated funds.

Pub. L. 108-487, title VI, §613, Dec. 23, 2004, 118 Stat. 3959, as amended by Pub. L. 109-364, div. A, title IX, §944(a)(2), (b)-(e), Oct. 17, 2006, 120 Stat. 2366, provided that Secretary of Defense, in coordination with Director of National Intelligence, shall conduct five-year pilot project to assess feasibility and advisability of establishing Civilian Linguist Reserve Corps comprised of United States citizens with advanced levels of proficiency in foreign languages who would be available upon the call of the Secretary to perform such service or duties with respect to such foreign languages in the intelligence community as the Secretary may specify and provided that the Secretary shall submit final report on project to Congress six months after completion of project.

§ 3323. Eligibility for incentive awards**(a) Scope of authority with respect to Federal employees and members of Armed Forces**

The Director of Central Intelligence may exercise the authority granted in section 4503 of title 5, with respect to Federal employees and members of the Armed Forces detailed or assigned to the Central Intelligence Agency or to the Intelligence Community Staff, in the same manner as such authority may be exercised with respect to the personnel of the Central Intelligence Agency and the Intelligence Community Staff.

(b) Time for exercise of authority

The authority granted by subsection (a) of this section may be exercised with respect to Federal employees or members of the Armed Forces detailed or assigned to the Central Intelligence Agency or to the Intelligence Community Staff on or after a date five years before December 9, 1983.

(c) Exercise of authority with respect to members of Armed Forces assigned to foreign intelligence duties

During fiscal year 1987, the Director of Central Intelligence may exercise the authority granted in section 4503(2) of title 5 with respect to members of the Armed Forces who are assigned to foreign intelligence duties at the time of the conduct which gives rise to the exercise of such authority.

(d) Payment and acceptance of award

An award made by the Director of Central Intelligence to an employee or member of the Armed Forces under the authority of section 4503 of title 5 or this section may be paid and accepted notwithstanding—

(1) section 5536 of title 5; and

(2) the death, separation, or retirement of the employee or the member of the Armed Forces whose conduct gave rise to the award, or the assignment of such member to duties other than foreign intelligence duties.

(Pub. L. 98-215, title IV, §402, Dec. 9, 1983, 97 Stat. 1477; Pub. L. 99-569, title V, §503, Oct. 27, 1986, 100 Stat. 3198.)

Editorial Notes**CODIFICATION**

Section was formerly classified to section 403e-1 of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

1986—Subsecs. (c), (d). Pub. L. 99-569 added subsecs. (c) and (d).

Statutory Notes and Related Subsidiaries**CHANGE OF NAME**

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 3001 of this title.

§ 3324. Prohibition on using journalists as agents or assets**(a) Policy**

It is the policy of the United States that an element of the Intelligence Community may not use as an agent or asset for the purposes of collecting intelligence any individual who—

(1) is authorized by contract or by the issuance of press credentials to represent himself or herself, either in the United States or

abroad, as a correspondent of a United States news media organization; or

(2) is officially recognized by a foreign government as a representative of a United States media organization.

(b) Waiver

Pursuant to such procedures as the President may prescribe, the President or the Director of Central Intelligence may waive subsection (a) in the case of an individual if the President or the Director, as the case may be, makes a written determination that the waiver is necessary to address the overriding national security interest of the United States. The Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate shall be notified of any waiver under this subsection.

(c) Voluntary cooperation

Subsection (a) shall not be construed to prohibit the voluntary cooperation of any person who is aware that the cooperation is being provided to an element of the United States Intelligence Community.

(Pub. L. 104-293, title III, §309, Oct. 11, 1996, 110 Stat. 3467.)

Editorial Notes**CODIFICATION**

Section was formerly classified to section 403-7 of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries**CHANGE OF NAME**

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 3001 of this title.

§ 3325. Reaffirmation of longstanding prohibition against drug trafficking by employees of the intelligence community**(a) Finding**

Congress finds that longstanding statutes, regulations, and policies of the United States prohibit employees, agents, and assets of the elements of the intelligence community, and of every other Federal department and agency, from engaging in the illegal manufacture, purchase, sale, transport, and distribution of drugs.

(b) Obligation of employees of intelligence community

Any employee of the intelligence community having knowledge of a fact or circumstance that reasonably indicates that an employee, agent, or asset of an element of the intelligence community is involved in any activity that violates a statute, regulation, or policy described in subsection (a) shall report such knowledge to an appropriate official.

(c) Intelligence community defined

In this section, the term “intelligence community” has the meaning given that term in section 3003(4) of this title.

(Pub. L. 106–120, title III, §313, Dec. 3, 1999, 113 Stat. 1615.)

Editorial Notes**CODIFICATION**

Section was formerly classified to section 403-8 of this title prior to editorial reclassification and renumbering as this section.

§ 3326. Limitation of expenditure of funds appropriated for Department of Defense intelligence programs

During the current fiscal year and hereafter, none of the funds appropriated for intelligence programs to the Department of Defense which are transferred to another Federal agency for execution shall be expended by the Department of Defense in any fiscal year in excess of amounts required for expenditure during such fiscal year by the Federal agency to which such funds are transferred.

(Pub. L. 102–172, title VIII, §8089, Nov. 26, 1991, 105 Stat. 1193.)

Editorial Notes**CODIFICATION**

Section was formerly classified as a note under section 414 of this title prior to editorial reclassification as this section.

§ 3327. Limitation on transfer of funds between CIA and Department of Defense; congressional notification required

During the current fiscal year and thereafter, no funds may be made available through transfer, reprogramming, or other means between the Central Intelligence Agency and the Department of Defense for any intelligence or special activity different from that previously justified to the Congress unless the Director of Central Intelligence or the Secretary of Defense has notified the House and Senate Appropriations Committees of the intent to make such funds available for such activity.

(Pub. L. 103–139, title VIII, §8107, Nov. 11, 1993, 107 Stat. 1464.)

Editorial Notes**CODIFICATION**

Section was formerly classified as a note under section 414 of this title prior to editorial reclassification as this section.

Statutory Notes and Related Subsidiaries**CHANGE OF NAME**

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of

the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of this title.

SIMILAR PROVISIONS

Provisions similar to those in this section were contained in the following prior appropriation acts:

Pub. L. 102–396, title IX, §9014, Oct. 6, 1992, 106 Stat. 1903.

Pub. L. 102–172, title VIII, §8014, Nov. 26, 1991, 105 Stat. 1174.

Pub. L. 101–511, title VIII, §8015, Nov. 5, 1990, 104 Stat. 1878.

Pub. L. 101–165, title IX, §9022, Nov. 21, 1989, 103 Stat. 1134.

Pub. L. 100–463, title VIII, §8035, Oct. 1, 1988, 102 Stat. 2270–23.

Pub. L. 100–202, §101(b) [title VIII, §8037], Dec. 22, 1987, 101 Stat. 1329–43, 1329–68.

§ 3328. Study or plan of surrender; use of appropriations

No part of the funds appropriated in any act shall be used to pay (1) any person, firm, or corporation, or any combinations of persons, firms, or corporations, to conduct a study or to plan when and how or in what circumstances the Government of the United States should surrender this country and its people to any foreign power, (2) the salary or compensation of any employee or official of the Government of the United States who proposes or contracts or who has entered into contracts for the making of studies or plans for the surrender by the Government of the United States of this country and its people to any foreign power in any event or under any circumstances.

(Pub. L. 85–766, ch. XVI, §1602, Aug. 27, 1958, 72 Stat. 884.)

Editorial Notes**CODIFICATION**

Section was formerly classified to section 407 of this title prior to editorial reclassification and renumbering as this section.

§ 3329. Intelligence community contracting**(a) In general**

The Director of National Intelligence shall direct that elements of the intelligence community, whenever compatible with the national security interests of the United States and consistent with the operational and security concerns related to the conduct of intelligence activities, and where fiscally sound, shall award contracts in a manner that would maximize the procurement of products in the United States.

(b) Intelligence community defined

In this section, the term “intelligence community” has the meaning given that term in section 3003(4) of this title.

(Pub. L. 102–183, title IV, §403, Dec. 4, 1991, 105 Stat. 1267; Pub. L. 111–259, title VIII, §810, Oct. 7, 2010, 124 Stat. 2750.)

Editorial Notes**CODIFICATION**

Section was formerly classified to section 403–2 of this title prior to editorial reclassification and renumbering as this section.

PRIOR PROVISIONS

Provisions similar to those in this section were contained in the following prior authorization act: Pub. L. 102-88, title IV, § 404, Aug. 14, 1991, 105 Stat. 434.

AMENDMENTS

2010—Pub. L. 111-259 added subsec. (b), designated existing provisions as subsec. (a), inserted heading, substituted “Director of National Intelligence” for “Director of Central Intelligence” and “intelligence community” for “Intelligence Community”, and struck out at end “For purposes of this provision, the term ‘Intelligence Community’ has the same meaning as set forth in paragraph 3.4(f) of Executive Order 12333, dated December 4, 1981, or successor orders.”

Statutory Notes and Related Subsidiaries

ENHANCED PROCUREMENT AUTHORITY TO MANAGE
SUPPLY CHAIN RISK

Pub. L. 112-87, title III, § 309, Jan. 3, 2012, 125 Stat. 1883, formerly set out as a note under this section, was transferred to section 3334e of this title.

§ 3330. Reports to the intelligence community on penetrations of networks and information systems of certain contractors**(a) Procedures for reporting penetrations**

The Director of National Intelligence shall establish procedures that require each cleared intelligence contractor to report to an element of the intelligence community designated by the Director for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) Networks and information systems subject to reporting

The Director of National Intelligence shall, in consultation with appropriate officials, establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

(c) Procedure requirements**(1) Rapid reporting**

The procedures established pursuant to subsection (a) shall require each cleared intelligence contractor to rapidly report to an element of the intelligence community designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following:

(A) A description of the technique or method used in such penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration.

(C) A summary of information created by or for such element in connection with any program of such element that has been potentially compromised due to such penetration.

(2) Access to equipment and information by intelligence community personnel

The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for intelligence community personnel to, upon request, obtain access to equipment or information of a cleared intelligence contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor;

(B) provide that a cleared intelligence contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for an element of the intelligence community in connection with any intelligence community program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated; and

(C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person (other than the name of the suspected perpetrator of the penetration).

(3) Limitation on dissemination of certain information

The procedures established pursuant to subsection (a) shall prohibit the dissemination outside the intelligence community of information obtained or derived through such procedures that is not created by or for the intelligence community except—

(A) with the approval of the contractor providing such information;

(B) to the congressional intelligence committees or the Subcommittees on Defense of the Committees on Appropriations of the House of Representatives and the Senate for such committees and such Subcommittees to perform oversight; or

(C) to law enforcement agencies to investigate a penetration reported under this section.

(d) Issuance of procedures and establishment of criteria**(1) In general**

Not later than 90 days after July 7, 2014, the Director of National Intelligence shall establish the procedures required under subsection (a) and the criteria required under subsection (b).

(2) Applicability date

The requirements of this section shall apply on the date on which the Director of National Intelligence establishes the procedures required under this section.

(e) Coordination with the Secretary of Defense to prevent duplicate reporting

Not later than 180 days after July 7, 2014, the Director of National Intelligence and the Secretary of Defense shall establish procedures to permit a contractor that is a cleared intelligence contractor and a cleared defense contractor under section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112-239; 10 U.S.C. 2224 note) to submit a single report that satisfies the requirements of this section and such section 941 for an incident of penetration of network or information system.

(f) Definitions

In this section:

(1) Cleared intelligence contractor

The term “cleared intelligence contractor” means a private entity granted clearance by the Director of National Intelligence or the head of an element of the intelligence community to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of an element of the intelligence community.

(2) Covered network

The term “covered network” means a network or information system of a cleared intelligence contractor that contains or processes information created by or for an element of the intelligence community with respect to which such contractor is required to apply enhanced protection.

(g) Savings clauses

Nothing in this section shall be construed to alter or limit any otherwise authorized access by government personnel to networks or information systems owned or operated by a contractor that processes or stores government data.

(Pub. L. 113–126, title III, §325, July 7, 2014, 128 Stat. 1402.)

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 2 of Pub. L. 113–126, set out as a note under section 3003 of this title.

§ 3331. Management of intelligence community personnel**(a) Multi-sector workforce initiative****(1) Requirement**

Beginning on October 1, 2018, the Director of National Intelligence shall improve management of the workforce of the intelligence community by enabling elements of the intelligence community to build and maintain an appropriate mix between employees of the United States Government and core contractors.

(2) Briefing to Congress

Not later than July 1, 2017, and each 120 days thereafter until July 1, 2018, the Director of National Intelligence shall brief the congressional intelligence committees on the initiative required by paragraph (1).

(b) Management based on workload requirements and authorized funding**(1) In general**

Beginning on October 1, 2018, the personnel levels of the intelligence community shall be managed each fiscal year on the basis of—

(A) the workload required to carry out the functions and activities of the intelligence community; and

(B) the funds made available to the intelligence community in accordance with section 3094 of this title.

(2) Prohibition on constraints or limitations

Beginning on October 1, 2018, the management of such personnel in the intelligence community in any fiscal year shall not be subject to an externally imposed constraint or limitation expressed in terms of man years, end strength, full-time equivalent positions, or maximum number of employees.

(c) Briefing and report to Congress

Not later than 180 days after May 5, 2017, the Director of National Intelligence shall issue a written report and provide a briefing to the congressional intelligence committees on—

(1) the methodology used to calculate the number of civilian and contractor full-time equivalent positions in the intelligence community;

(2) the cost analysis tool used to calculate personnel costs in the intelligence community; and

(3) the plans of the Director of National Intelligence and the head of each element of the intelligence community to implement a multi-sector workforce as required by subsections (a) and (b).

(d) Report

Not later than 240 days after May 5, 2017, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a written report on the accuracy of intelligence community data for the numbers and costs associated with the civilian and contractor workforce in each element of the intelligence community.

(Pub. L. 115–31, div. N, title III, §306, May 5, 2017, 131 Stat. 812.)

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3332. Guidance and reporting requirement regarding the interactions between the intelligence community and entertainment industry**(a) Definitions**

In this section:

(1) Engagement

The term “engagement”—

(A) means any significant interaction between an element of the intelligence community and an entertainment industry entity for the purposes of contributing to an entertainment product intended to be heard, read, viewed, or otherwise experienced by the public; and

(B) does not include routine inquiries made by the press or news media to the public affairs office of an intelligence community.

(2) Entertainment industry entity

The term “entertainment industry entity” means an entity that creates, produces, pro-

motes, or distributes a work of entertainment intended to be heard, read, viewed, or otherwise experienced by an audience, including—

(A) theater productions, motion pictures, radio broadcasts, television broadcasts, podcasts, webcasts, other sound or visual recording, music, or dance;

(B) books and other published material; and

(C) such other entertainment activity, as determined by the Director of National Intelligence.

(b) Director of National Intelligence guidance

(1) In general

Not later than 180 days after May 5, 2017, the Director of National Intelligence shall issue, and release to the public, guidance regarding engagements by elements of the intelligence community with entertainment industry entities.

(2) Criteria

The guidance required by paragraph (1) shall permit an element of the intelligence community to conduct engagements, if the head of the element, or a designee of such head, provides prior approval.

(c) Information on prior year engagements

At the written request of either of the congressional intelligence committees, the Director of National Intelligence shall submit to such committees information with respect to engagements occurring during the calendar year prior to the year during which such request is made. Such information may include—

(1) a description of the nature and duration of each such engagement;

(2) the cost incurred by the United States Government for each such engagement;

(3) a description of the benefits to the United States Government for each such engagement;

(4) a determination of whether any information was declassified, and whether any classified information was improperly disclosed, for each such engagement; and

(5) a description of the work produced through each such engagement.

(Pub. L. 115–31, div. N, title III, § 308, May 5, 2017, 131 Stat. 813; Pub. L. 116–92, div. E, title LVII, § 5701(d), Dec. 20, 2019, 133 Stat. 2160.)

Editorial Notes

AMENDMENTS

2019—Subsec. (b)(2). Pub. L. 116–92, § 5701(d)(1), struck out subpar. (A) designation before “permit an element”, substituted “shall” for “shall—” and “approval.” for “approval; and”, and struck out subpar. (B) which read as follows: “require an unclassified annual report to the congressional intelligence committees regarding engagements.”

Subsec. (c). Pub. L. 116–92, § 5701(d)(2), added subsec. (c) and struck out former subsec. (c) which related to the annual report to the congressional intelligence committees regarding engagements.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in

this section, see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3333. Joint facilities certification

(a) Findings

Congress finds the following:

(1) The Director of National Intelligence set a strategic goal to use joint facilities as a means to save costs by consolidating administrative and support functions across multiple elements of the intelligence community.

(2) The use of joint facilities provides more opportunities for operational collaboration and information sharing among elements of the intelligence community.

(b) Certification

Before an element of the intelligence community purchases, leases, or constructs a new facility that is 20,000 square feet or larger, the head of that element of the intelligence community shall submit to the Director of National Intelligence—

(1) a written certification that, to the best of the knowledge of the head of such element, all prospective joint facilities in the vicinity have been considered and the element is unable to identify a joint facility that meets the operational requirements of such element; and

(2) a written statement listing the reasons for not participating in the prospective joint facilities considered by the element.

(Pub. L. 115–31, div. N, title VI, § 604, May 5, 2017, 131 Stat. 830.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3334. Intelligence community public-private talent exchange

(a) Policies, processes, and procedures required

(1) In general

Not later than 270 days after December 20, 2019, the Director of National Intelligence shall develop policies, processes, and procedures to facilitate the rotation of personnel of the intelligence community to the private sector, and personnel from the private sector to the intelligence community.

(2) Focus areas

The Director shall ensure that the policies, processes, and procedures developed pursuant to paragraph (1) require exchanges under this section that relate to intelligence or counterintelligence with a focus on rotations described in such paragraph with private-sector organizations in the following fields:

(A) Finance.

(B) Acquisition.

(C) Biotechnology.

(D) Computing.

(E) Artificial intelligence.

(F) Business process innovation and entrepreneurship.

(G) Cybersecurity.

(H) Materials and manufacturing.

(I) Any other technology or research field the Director determines relevant to meet evolving national security threats in technology sectors.

(b) Detail authority

Under policies developed by the Director pursuant to subsection (a), pursuant to a written agreement with a private-sector organization, and with the consent of the employee, a head of an element of the intelligence community may arrange for the temporary detail of an employee of such element to such private-sector organization, or from such private-sector organization to such element under this section.

(c) Agreements

(1) In general

A head of an element of the intelligence community exercising the authority of the head under subsection (a) shall provide for a written agreement among the element of the intelligence community, the private-sector organization, and the employee concerned regarding the terms and conditions of the employee's detail under this section. The agreement—

(A) shall require that the employee of the element, upon completion of the detail, serve in the element, or elsewhere in the civil service if approved by the head of the element, for a period that is at least equal to the length of the detail;

(B) shall provide that if the employee of the element fails to carry out the agreement, such employee shall be liable to the United States for payment of all nonsalary and benefit expenses of the detail, unless that failure was for good and sufficient reason, as determined by the head of the element;

(C) shall contain language informing such employee of the prohibition on sharing, using, or otherwise improperly handling classified or unclassified nonpublic information for the benefit or advantage of the private-sector organization;

(D) shall contain language governing the handling of classified information by such employee during the detail; and

(E) shall contain language requiring the employee to acknowledge the obligations of the employee under section 1905 of title 18.

(2) Amount of liability

An amount for which an employee is liable under paragraph (1) shall be treated as a debt due the United States.

(3) Waiver

The head of an element of the intelligence community may waive, in whole or in part, collection of a debt described in paragraph (2) based on a determination that the collection would be against equity and good conscience and not in the best interests of the United States, after taking into account any indication of fraud, misrepresentation, fault, or lack of good faith on the part of the employee.

(d) Termination

A detail under this section may, at any time and for any reason, be terminated by the head of

the element of the intelligence community concerned or the private-sector organization concerned.

(e) Duration

(1) In general

A detail under this section shall be for a period of not less than 3 months and not more than 2 years, renewable up to a total of 5 years.

(2) Longer periods

A detail under this section may be for a period in excess of 2 years, but not more than 5 years, if the head of the element making the detail determines that such detail is necessary to meet critical mission or program requirements.

(3) Limitation

No employee of an element of the intelligence community may be detailed under this section for more than a total of 5 years, inclusive of all such details.

(f) Status of Federal employees detailed to private-sector organizations

(1) In general

An employee of an element of the intelligence community who is detailed to a private-sector organization under this section shall be considered, during the period of detail, to be on a regular work assignment in the element. The written agreement established under subsection (c)(1) shall address the specific terms and conditions related to the employee's continued status as a Federal employee.

(2) Requirements

In establishing a temporary detail of an employee of an element of the intelligence community to a private-sector organization, the head of the element shall—

(A) certify that the temporary detail of such employee shall not have an adverse or negative impact on mission attainment or organizational capabilities associated with the detail; and

(B) in the case of an element of the intelligence community in the Department of Defense, ensure that the normal duties and functions of such employees are not, as a result of and during the course of such temporary detail, performed or augmented by contractor personnel in violation of the provisions of section 2461 of title 10.

(g) Terms and conditions for private-sector employees

An employee of a private-sector organization who is detailed to an element of the intelligence community under this section—

(1) shall continue to receive pay and benefits from the private-sector organization from which such employee is detailed and shall not receive pay or benefits from the element, except as provided in paragraph (2);

(2) is deemed to be an employee of the element for the purposes of—

(A) chapters 73 and 81 of title 5;

(B) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18;

(C) sections 1343, 1344, and 1349(b) of title 31;

(D) chapter 171 of title 28 (commonly known as the “Federal Tort Claims Act”) and any other Federal tort liability statute;

(E) the Ethics in Government Act of 1978 (5 U.S.C. App.);¹ and

(F) chapter 21 of title 41;

(3) may perform work that is considered inherently governmental in nature only when requested in writing by the head of the element;

(4) may not be used to circumvent any limitation or restriction on the size of the workforce of the element;

(5) shall be subject to the same requirements applicable to an employee performing the same functions and duties proposed for performance by the private-sector employee;

(6) in the case of an element of the intelligence community in the Department of Defense, may not be used to circumvent the provisions of section 2461 of title 10; and

(7) shall not have access to any trade secrets or proprietary information which is of commercial value or competitive advantage to the private-sector organization from which such employee is detailed.

(h) Prohibition against charging certain costs to the Federal Government

A private-sector organization may not charge an element of the intelligence community or any other agency of the Federal Government, as direct costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee detailed to an element of the intelligence community under this section for the period of the detail and any subsequent renewal periods.

(i) Organizational conflicts of interest

(1) In general

A private-sector organization that temporarily details a member of its workforce to an element of the intelligence community or that accepts the temporary detail of a member of the intelligence community shall not be considered to have an organizational conflict of interest with the element of the intelligence community solely because of participation in the program established under this section.

(2) Identification of conflicts of interest

If the identification of an organizational conflict of interest arises based on the particular facts surrounding an individual’s participation in the program established under this section and the nature of any contract, then the heads of intelligence community elements shall implement a system to avoid, neutralize, or mitigate any such organizational conflicts of interest.

(j)² Additional administrative matters

In carrying out this section, the Director, pursuant to procedures developed under subsection (a)—

(1) shall, to the degree practicable, ensure that small business concerns are represented

with respect to details authorized by this section;

(2) may, notwithstanding any other provision of law, establish criteria for elements of the intelligence community to use appropriated funds to reimburse small business concerns for the salaries and benefits of its employees during the periods when the small business concern agrees to detail its employees to the intelligence community under this section;

(3) shall take into consideration the question of how details under this section might best be used to help meet the needs of the intelligence community, including with respect to the training of employees;

(4) shall take into consideration areas of private-sector expertise that are critical to the intelligence community; and

(5) shall establish oversight mechanisms to determine whether the public-private exchange authorized by this section improves the efficiency and effectiveness of the intelligence community.

(j)² Definitions

In this section:

(1) Detail

The term “detail” means, as appropriate in the context in which such term is used—

(A) the assignment or loan of an employee of an element of the intelligence community to a private-sector organization without a change of position from the intelligence community element that employs the individual; or

(B) the assignment or loan of an employee of a private-sector organization to an element of the intelligence community without a change of position from the private-sector organization that employs the individual.

(2) Private-sector organization

The term “private-sector organization” means—

(A) a for-profit organization; or
(B) a not-for-profit organization.

(3) Small business concern

The term “small business concern” has the meaning given such term in section 3703(e)(2) of title 5.

(Pub. L. 116–92, div. E, title LIII, § 5306, Dec. 20, 2019, 133 Stat. 2122; Pub. L. 118–159, div. F, title LXV, § 6506(a)–(d), Dec. 23, 2024, 138 Stat. 2496, 2497.)

Editorial Notes

REFERENCES IN TEXT

The Ethics in Government Act of 1978, referred to in subsec. (g)(2)(E), is Pub. L. 95–521, Oct. 26, 1978, 92 Stat. 1824. Titles I, IV, and V of the Act were classified principally to the Appendix to Title 5, Government Organization and Employees, and were substantially repealed and restated in chapter 131 (§ 13101 et seq.) of Title 5 by Pub. L. 117–286, §§ 3(c), 7, Dec. 27, 2022, 136 Stat. 4266, 4361. For complete classification of this Act to the Code, see Tables. For disposition of sections of the Act into chapter 131 of Title 5, see Disposition Table preceding section 101 of Title 5.

¹ See References in Text note below.

² So in original. There are two subssecs. (j).

AMENDMENTS

2024—Subsec. (a). Pub. L. 118–159, § 6506(a), designated existing provisions as par. (1), inserted heading, and added par. (2).

Subsec. (e)(1), (2). Pub. L. 118–159, § 6506(b), substituted “5 years” for “3 years”.

Subsec. (g)(7). Pub. L. 118–159, § 6506(c), added par. (7).

Subsecs. (i), (j). Pub. L. 118–159, § 6506(d), added subsec. (i) and redesignated former subsec. (i) as (j) relating to additional administrative matters.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3334a. Transfer of National Intelligence University to the Office of the Director of National Intelligence

(a) Transfer

Upon the submission of the joint certifications under subsection (b)(1), the Secretary of Defense and the Director of National Intelligence shall take such actions that the Director determines necessary to transfer the National Intelligence University from the Defense Intelligence Agency to the Director of National Intelligence.

(b) Joint certifications

(1) Requirement

Except as provided by paragraph (2), as soon as practicable after December 20, 2019, but not later than 18 months after December 20, 2019, the Secretary of Defense and the Director of National Intelligence shall jointly submit to the appropriate congressional committees written certifications of each of the following:

(A) The Middle States Commission on Higher Education has provided regional academic accreditation for the National Intelligence University before the date of the certification, or will provide such academic accreditation as of the date on which the University is transferred under subsection (a).

(B) Members of the Armed Forces attending the University will be eligible to receive credit for Phase I joint professional military education.

(C) The Secretary of Education has informed the Director of National Intelligence that the Secretary has recommended approval of the degrees to be conferred pursuant to section 3227a(b) of this title or will provide such recommended approval as of the date on which the University is transferred under subsection (a).

(D) The Director of National Intelligence, in collaboration with the Secretary of Defense, has established an appropriate governance model for the University.

(E) The Secretary of Defense shall use the University to provide personnel of the Department of Defense with advanced intelligence education.

(2) Failure to certify

(A) Actions required

If the Secretary of Defense and the Director of National Intelligence fail to submit

the certifications under paragraph (1) by the date specified in such paragraph, the Secretary and the Director shall—

(i) jointly submit to the appropriate congressional committees a report on such failure by not later than 21 months after December 20, 2019; and

(ii) jointly submit such certifications as soon as practicable.

(B) Contents of report

The report under subparagraph (A)(i) shall contain the following:

(i) A description of the progress made toward fulfilling the conditions described in such paragraph as of the date of the report.

(ii) A description of any obstacles preventing the fulfillment of such conditions.

(iii) The estimated dates of completion for the fulfillment of such conditions and the submission of the certifications.

(c) Briefing

Not later than 90 days after December 20, 2019, the Director of National Intelligence, the Director of the Defense Intelligence Agency, and the President of the National Intelligence University shall jointly provide to the appropriate congressional committees a briefing on the plan to carry out the transfer under subsection (a), including with respect to—

(1) ensuring the provision of services to all elements of the intelligence community;

(2) employing a military cadre at the University; and

(3) addressing the current accreditation status of the National Intelligence University with the Middle States Commission on Higher Education.

(d) Cost estimates of transfer

(1) Requirement

Not later than 90 days after December 20, 2019, the Secretary of Defense and the Director of National Intelligence shall jointly submit to the appropriate congressional committees an estimate of—

(A) the annual costs of operating the National Intelligence University; and

(B) the costs to the Federal Government of transferring the National Intelligence University to the Director of National Intelligence.

(2) Inclusion of indirect costs

The estimate submitted under paragraph (1) shall include all indirect costs, including with respect to human resources, security, facilities, and information technology.

(e) Conforming repeal

(1) Omitted

(2) Effective date

The amendments made by paragraph (1) shall take effect on the date on which the Secretary of Defense and the Director of National Intelligence jointly submit the joint certifications under subsection (b)(1). The Secretary and the Director shall jointly notify the Law Revision Counsel of the House of Representa-

tives of the submission of the certifications so that the Law Revision Counsel may execute the amendments made by paragraph (1).

(f) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

- (A) the congressional intelligence committees; and
- (B) the Committees on Armed Services of the Senate and House of Representatives.

(2) Phase I joint professional military education

The term “Phase I joint professional military education” has the meaning given that term pursuant to section 2154 of title 10.

(Pub. L. 116–92, div. E, title LIII, § 5324, Dec. 20, 2019, 133 Stat. 2134; Pub. L. 116–260, div. W, title III, § 305(c), Dec. 27, 2020, 134 Stat. 2367.)

Editorial Notes

CODIFICATION

Section is comprised of section 5324 of Pub. L. 116–92. Subsec. (e)(1) of section 5324 of Pub. L. 116–92 repealed section 2161 of Title 10, Armed Forces, and amended the analysis preceding section 2161 of Title 10.

AMENDMENTS

2020—Subsec. (b)(1)(C). Pub. L. 116–260, § 305(c)(1), substituted “section 3227a(b) of this title” for “subsection (e)(2)”.

Subsecs. (e) to (h). Pub. L. 116–260, § 305(c)(2), (3), redesignated subsecs. (g) and (h) as (e) and (f), respectively, and struck out former subsecs. (e) and (f) which related to degree-granting authority and congressional notification requirements, respectively.

Statutory Notes and Related Subsidiaries

DEFINITIONS

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

§ 3334b. Collection, analysis, and dissemination of workforce data

(a) Omitted

(b) Initial reporting

(1) In general

Not later than 180 days after December 20, 2019, the Director of National Intelligence shall make available to the public, the appropriate congressional committees, and the workforce of the intelligence community a report which includes aggregate demographic data and other information regarding the diversity and inclusion efforts of the workforce of the intelligence community.

(2) Contents

A report made available under paragraph (1)—

- (A) shall include unclassified reports and barrier analyses relating to diversity and inclusion efforts;
- (B) shall include aggregate demographic data—

- (i) by segment of the workforce of the intelligence community and grade or rank;

- (ii) relating to attrition and promotion rates;

- (iii) that addresses the compliance of the intelligence community with validated inclusion metrics, such as the New Inclusion Quotient index score; and

- (iv) that provides demographic comparisons to the relevant nongovernmental labor force and the relevant civilian labor force;

(C) shall include an analysis of applicant flow data, including the percentage and level of positions for which data are collected, and a discussion of any resulting policy changes or recommendations;

(D) shall include demographic data relating to participants in professional development programs of the intelligence community and the rate of placement into senior positions for participants in such programs;

(E) shall include any voluntarily collected demographic data relating to the membership of any external advisory committee or board to which individuals in senior positions in the intelligence community appoint members; and

(F) may include data in proportions or percentages to account for concerns relating to the protection of classified information.

(c) Updates

Not later than March 31 of each year, the Director of National Intelligence shall provide a report (which may be provided as part of an annual report required under another provision of law) to the workforce of the intelligence community (including senior leadership), the public, and the appropriate congressional committees that includes—

- (1) demographic data and information on the status of diversity and inclusion efforts of the intelligence community, including demographic data relating to—

- (A) the average years of service;

- (B) the average number of years of service for each level in the General Schedule, Senior Executive Service, Senior Intelligence Service, or equivalent; and

- (C) career categories;

- (2) an analysis of applicant flow data, including the percentage and level of positions for which data are collected, and a discussion of any resulting policy changes or recommendations; and

- (3) demographic data relating to participants in professional development programs of the intelligence community and the rate of placement into senior positions for participants in such programs.

(d) Expand the collection and analysis of voluntary applicant flow data

(1) In general

The Director of National Intelligence shall develop a system to collect and analyze applicant flow data for as many positions within the intelligence community as practicable, in order to identify areas for improvement in at-

tracting diverse talent, with particular attention to senior and management positions.

(2) Phased implementation

The collection of applicant flow data may be implemented by the Director of National Intelligence in a phased approach commensurate with the resources available to the intelligence community.

(e) Identify additional categories for voluntary data collection of current employees

(1) In general

The Director of National Intelligence may submit to the Office of Management and Budget and to the appropriate congressional committees a recommendation regarding whether the intelligence community should voluntarily collect more detailed data on demographic categories in addition to the race and ethnicity categories specified in the statistical policy directive issued by the Office of Management and Budget entitled “Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity”.

(2) Process

In making a recommendation under paragraph (1), the Director of National Intelligence shall—

(A) engage in close consultation with internal stakeholders, such as employee resource or affinity groups;

(B) ensure that there is clear communication with the workforce of the intelligence community—

(i) to explain the purpose of the potential collection of such data; and

(ii) regarding legal protections relating to any anticipated use of such data; and

(C) ensure adherence to relevant standards and guidance issued by the Federal Government.

(f) Definitions

In this section:

(1) Applicant flow data

The term “applicant flow data” means data that tracks the rate of applications for job positions among demographic categories.

(2) Appropriate congressional committees

The term “appropriate congressional committees” means—

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

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

(3) Diversity

The term “diversity” means diversity of persons based on gender, race, ethnicity, disability status, veteran status, sexual orientation, gender identity, national origin, and other demographic categories.

(Pub. L. 116–92, div. E, title LVII, § 5704, Dec. 20, 2019, 133 Stat. 2162; Pub. L. 117–103, div. X, title VIII, § 802, Mar. 15, 2022, 136 Stat. 1011; Pub. L. 117–263, div. F, title LXVIII, § 6824(b)(1), Dec. 23, 2022, 136 Stat. 3615.)

Editorial Notes

CODIFICATION

Section is comprised of section 5704 of Pub. L. 116–92. Subsec. (a) of section 5704 of Pub. L. 116–92 amended section 3050 of this title.

AMENDMENTS

2022—Subsec. (b)(1). Pub. L. 117–263 struck out “, and subject to paragraph (3)” after “Not later than 180 days after December 20, 2019”.

Subsec. (c). Pub. L. 117–103, § 802(1), substituted “Not later than March 31 of each year, the Director of National Intelligence shall provide a report” for “After making available a report under subsection (b), the Director of National Intelligence shall annually provide a report” in introductory provisions.

Subsec. (c)(1). Pub. L. 117–103, § 802(2), added par. (1) and struck out former par. (1) which read as follows: “demographic data and information on the status of diversity and inclusion efforts of the intelligence community”.

Statutory Notes and Related Subsidiaries

EXPANSION OF INTELLIGENCE COMMUNITY RECRUITMENT EFFORTS

Pub. L. 116–92, div. E, title LXIII, § 6316, Dec. 20, 2019, 133 Stat. 2195, as amended by Pub. L. 117–263, div. F, title LXVIII, § 6824(b)(2), Dec. 23, 2022, 136 Stat. 3615, provided that: “In order to further increase the diversity of the intelligence community workforce, not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Director of National Intelligence, in consultation with heads of elements of the Intelligence Community, shall create, implement, and submit to the congressional intelligence committees a written plan to ensure that rural and underrepresented regions are more fully and consistently represented in such elements’ employment recruitment efforts. Upon receipt of the plan, the congressional intelligence committees shall have 60 days to submit comments to the Director of National Intelligence before such plan shall be implemented.”

[For definitions of “intelligence community” and “congressional intelligence committees” as used in section 6316 of Pub. L. 116–92, set out above, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.]

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3334c. Assessment of homeland security vulnerabilities associated with certain retired and former personnel of the intelligence community

(a) Assessment required

Not later than the date that is 120 days after submission of the report required under section 5703,¹ and annually thereafter, the Director of National Intelligence, in coordination with the Under Secretary of Homeland Security for Intelligence and Analysis, the Director of the Federal Bureau of Investigation, the Director of the Cen-

¹ See References in Text note below.

tral Intelligence Agency, and the Director of the Defense Counterintelligence and Security Agency, shall submit to the appropriate congressional committees an assessment of the homeland security vulnerabilities associated with retired and former personnel of the intelligence community providing covered intelligence assistance.

(b) Form

The assessment under subsection (a) may be submitted in classified form.

(c) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

(A) the congressional intelligence committees;

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

(C) the Committee on Homeland Security of the House of Representatives.

(2) Covered intelligence assistance

The term “covered intelligence assistance” has the meaning given that term in section 5703.¹

(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 [sic]

“(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” as used in this section, 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) Requirement to provide cyber protection support

(1) In general

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

(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 be-

cause 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 congressional 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; Pub. L. 117-263, div. F, title LXIII, § 6308(a), Dec. 23, 2022, 136 Stat. 3506.)

Editorial Notes

AMENDMENTS

2022—Subsec. (b). Pub. L. 117-263, § 6308(a)(2), substituted “Requirement” for “Authority” in heading.

Subsec. (b)(1). Pub. L. 117-263, § 6308(a)(1), substituted “shall offer” for “may provide” and inserted at end “and shall provide such support to any such personnel who request”.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, 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 3552 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 committees that includes a summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why they were not reasonably available to reduce supply chain risk.

(d) Delegation

The head of a covered agency may not delegate the authority provided in subsection (b) or the responsibility to make a determination under subsection (c) to an official below the level of the service acquisition executive for the agency concerned.

(e) Savings

The authority under this section is in addition to any other authority under any other provision of law. The authority under this section shall not be construed to alter or effect the exercise of any other provision of law.

(f) Effective date

The requirements of this section shall take effect on the date that is 180 days after January 3, 2012, and shall apply to contracts that are awarded on or after such date.

(Pub. L. 112-87, title III, § 309, Jan. 3, 2012, 125 Stat. 1883; Pub. L. 116-92, div. E, title LXIII, § 6309, Dec. 20, 2019, 133 Stat. 2190; Pub. L. 117-263, div. F, title LXVIII, § 6824(c), Dec. 23, 2022, 136 Stat. 3615.)

Editorial Notes

CODIFICATION

Section was formerly set out as a note under section 3329 of this title.

AMENDMENTS

2022—Subsec. (a)(5). Pub. L. 117-263 substituted “section 3552” for “section 3542(b)”.

2019—Subsec. (g). Pub. L. 116-92 struck out subsec. (g). Prior to amendment, text read as follows: “The authority provided in this section shall expire on the date that section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383; 10 U.S.C. 2304 note) expires.”

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 2 of Pub. L. 112-87, set out as a note under section 3003 of this title.

§ 3334f. Congressional notification of designation of covered intelligence officer as persona non grata

(a) Covered intelligence officer defined

In this section, the term “covered intelligence officer” means—

(1) a United States intelligence officer serving in a post in a foreign country; or

(2) a known or suspected foreign intelligence officer serving in a United States post.

(b) Requirement for reports

Not later than 72 hours after a covered intelligence officer is designated as a persona non grata, the Director of National Intelligence, in consultation with the Secretary of State, shall submit to the congressional intelligence committees, the Committee on Foreign Relations of the Senate, and the Committee on Foreign Affairs of the House of Representatives a notification of that designation. Each such notification shall include—

(1) the date of the designation;

(2) the basis for the designation; and

(3) a justification for the expulsion.

(Pub. L. 116-92, div. E, title LXVII, § 6719, Dec. 20, 2019, 133 Stat. 2229.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3334g. Reports on intelligence community loan repayment and related programs

(a) Sense of Congress

It is the sense of Congress that—

(1) there should be established, through the issuing of an Intelligence Community Directive or otherwise, an intelligence-community-wide program for student loan repayment, student loan forgiveness, financial counseling, and related matters, for employees of the intelligence community;

(2) creating such a program would enhance the ability of the elements of the intelligence community to recruit, hire, and retain highly qualified personnel, including with respect to mission-critical and hard-to-fill positions;

(3) such a program, including with respect to eligibility requirements, should be designed so

as to maximize the ability of the elements of the intelligence community to recruit, hire, and retain highly qualified personnel, including with respect to mission-critical and hard-to-fill positions; and

(4) to the extent possible, such a program should be uniform throughout the intelligence community and publicly promoted by each element of the intelligence community to both current employees of the element as well as to prospective employees of the element.

(b) Report on potential intelligence community-wide program

(1) In general

Not later than 180 days after December 20, 2019, the Director of National Intelligence, in cooperation with the heads of the elements of the intelligence community and the heads of any other appropriate department or agency of the Federal Government, shall submit to the congressional intelligence committees a report on potentially establishing and carrying out an intelligence-community-wide program for student loan repayment, student loan forgiveness, financial counseling, and related matters, as described in subsection (a).

(2) Matters included

The report under paragraph (1) shall include, at a minimum, the following:

(A) A description of the financial resources that the elements of the intelligence community would require to establish and initially carry out the program specified in paragraph (1).

(B) A description of the practical steps to establish and carry out such a program.

(C) The identification of any legislative action the Director determines necessary to establish and carry out such a program.

(Pub. L. 116–92, div. E, title LXVII, § 6725, Dec. 20, 2019, 133 Stat. 2234; Pub. L. 118–159, div. F, title LXIX, § 6901(e), Dec. 23, 2024, 138 Stat. 2517.)

Editorial Notes

AMENDMENTS

2024—Subsec. (c). Pub. L. 118–159 struck out subsec. (c) which required annual reports to Congress regarding various loan and financial counseling programs.

Statutory Notes and Related Subsidiaries

INTELLIGENCE COMMUNITY STUDENT LOAN REPAYMENT PROGRAMS

Pub. L. 116–260, div. W, title III, § 310, Dec. 27, 2020, 134 Stat. 2369, provided that:

“(a) SENSE OF CONGRESS.—It is the sense of Congress that—

“(1) student loan repayment programs are a crucial tool in attracting and retaining talented individuals to the intelligence community, particularly individuals from diverse backgrounds;

“(2) generous student loan repayment programs help the intelligence community compete with the private sector for talented employees;

“(3) departments and agencies containing elements of the intelligence community have authority to establish student loan repayment programs either under section 5379 of title 5, United States Code, or under the delegable authority of the Director of National Intelligence under section 102A(n)(1) of the National Security Act of 1947 (50 U.S.C. 3024(n)(1));

“(4) although the Director should use the authority under such section 102A(n)(1) sparingly, and should be exceedingly sparing in delegating such authority to an element of the intelligence community, the Director should approve well-predicated requests for such authority in the student loan repayment context if an element of the intelligence community can articulate an impediment to establishing or enhancing a program under section 5379 of title 5, United States Code; and

“(5) student loan repayment programs established by an element of the intelligence community should provide flexibility to intelligence community employees, including employees who pursue loan-financed education in the middle of their careers or after the day on which they first become intelligence community employees.

“(b) STUDENT LOAN REPAYMENT PROGRAM STANDARDS.—Not later than 180 days after the date of the enactment of this Act [Dec. 27, 2020], the Director of National Intelligence, or a designee of the Director who is an employee of the Office of the Director of National Intelligence, shall establish minimum standards for the repayment of student loans of employees of elements of the intelligence community by such elements of the intelligence community.

“(c) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the standards established under subsection (b). Such report shall include—

“(1) an explanation of why such minimum standards were established; and

“(2) how such standards advance the goals of—

“(A) attracting and retaining a talented intelligence community workforce;

“(B) competing with private sector companies for talented employees; and

“(C) promoting the development of a diverse workforce.

“(d) FAILURE TO MEET STANDARDS.—Not later than 180 days after the date on which the standards required under subsection (b) are established, the head of an element of the intelligence community that does not meet such standards shall submit to the appropriate congressional committees a report containing an explanation for why such element does not meet such standards and an identification of any additional authority or appropriations required to for the element to meet such standards.

“(e) SUBMITTAL OF REGULATIONS AND POLICIES TO CONGRESS.—Not later than 180 days after the date on which the standards required under subsection (b) are established, the head of an element of the intelligence community shall submit to the appropriate congressional committees a copy of all internal regulations and policies governing the student loan repayment program of that element as well as copies of such policies redacted to remove classified information.

“(f) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ‘appropriate congressional committees’ means—

“(1) the Permanent Select Committee on Intelligence of the House of Representatives;

“(2) the Select Committee on Intelligence of the Senate;

“(3) with respect to an element of the intelligence community within the Department of Defense, the Committees on Armed Services of the Senate and House of Representatives;

“(4) with respect to an element of the intelligence community within the Department of Justice, the Committees on the Judiciary of the Senate and House of Representatives;

“(5) with respect to an element of the intelligence community within the Department of Homeland Security, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives;

“(6) with respect to an element of the intelligence community within the Department of State, the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives;

“(7) with respect to an element of the intelligence community within the Department of Energy, the Committee on Energy and Natural Resources of the Senate and the Committee on Energy and Commerce of the House of Representatives; and

“(8) with respect to an element of the intelligence community within the Department of the Treasury, the Committee on Finance of the Senate and the Committee on Financial Services of the House of Representatives.

“(g) FORM OF REPORTS.—Each of the reports required under subsections (c) and (d) shall be submitted in unclassified form, but may contain a classified annex.”

[For definition of “intelligence community” as used in section 310 of div. W of Pub. L. 116-260, set out above, see section 2 of div. W of Pub. L. 116-260, set out as a note under section 3003 of this title.]

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3334h. Data collection on attrition in intelligence community

(a) Standards for data collection

(1) In general

Not later than 90 days after December 27, 2020, the Director of National Intelligence shall establish standards for collecting data relating to attrition in the intelligence community workforce across demographics, specialties, and length of service.

(2) Inclusion of certain candidates

The Director shall include, in the standards established under paragraph (1), standards for collecting data from candidates who accepted conditional offers of employment but chose to withdraw from the hiring process before entering into service, including data with respect to the reasons such candidates chose to withdraw.

(b) Collection of data

Not later than 120 days after December 27, 2020, each element of the intelligence community shall begin collecting data on workforce and candidate attrition in accordance with the standards established under subsection (a).

(Pub. L. 116-260, div. W, title III, § 306, Dec. 27, 2020, 134 Stat. 2367; Pub. L. 118-159, div. F, title LXIX, § 6901(f), Dec. 23, 2024, 138 Stat. 2517.)

Editorial Notes

AMENDMENTS

2024—Subsec. (c). Pub. L. 118-159 struck out subsec. (c) which required annual reports to Congress regarding workforce and candidate attrition in the intelligence community.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 2 of div. W of Pub. L. 116-260, set out as a note under section 3003 of this title.

§ 3334i. Seedling investment in next-generation microelectronics in support of artificial intelligence

(a) Findings

Congress finds that—

(1) developing faster, more energy efficient, and more resilient computing is important to the future of the national security of the United States and the leadership by the United States in artificial intelligence; and

(2) multidisciplinary teams co-designing microelectronics for artificial intelligence will lead to unprecedented capabilities that will help ensure that the United States maintains its superiority in this worldwide competition for economic and national security.

(b) Awards for research and development

The Director of National Intelligence, acting through the Director of the Intelligence Advanced Research Projects Activity, shall award contracts or grants, or enter into transactions other than contracts, to encourage microelectronics research.

(c) Use of funds

The Director shall award contracts or grants to, or enter into transactions other than contracts with, entities under subsection (b) to carry out any of the following:

(1) Advanced engineering and applied research into novel computing models, materials, devices, architectures, or algorithms to enable the advancement of artificial intelligence and machine learning.

(2) Research efforts to—

(A) overcome challenges with engineering and applied research of microelectronics, including with respect to the physical limits on transistors, electrical interconnects, and memory elements; or

(B) promote long-term advancements in computing technologies, including by fostering a unified and multidisciplinary approach encompassing research and development into algorithm design, computing architectures, microelectronic devices and circuits, and the chemistry and physics of new materials.

(3) Any other activity the Director determines would promote the development of microelectronics research.

(d) Award amounts

In awarding contracts or grants, or entering into transactions other than contracts, under subsection (b), the Director may award not more than a total of \$15,000,000.

(Pub. L. 116-260, div. W, title V, § 502, Dec. 27, 2020, 134 Stat. 2382.)

§ 3334j. Access to certain facilities of United States Government for assessment of anomalous health conditions

(a) Assessment

The Director of National Intelligence shall ensure that the elements of the intelligence community provide to individuals described in subsection (c) who are experiencing symptoms of anomalous health conditions timely access for

medical assessment to facilities of the United States Government with expertise in traumatic brain injury.

(b) Process for assessment and treatment

In carrying out subsection (a), the Director of National Intelligence shall coordinate with the Secretary of Defense and the heads of such Federal agencies as the Director considers appropriate to ensure that, by not later than 60 days after March 15, 2022, there is a process to provide the individuals described in subsection (c) with timely access to the National Intrepid Center of Excellence, an Intrepid Spirit Center, or an appropriate medical treatment facility for assessment as described in subsection (a) and, if necessary, treatment.

(c) Individuals described

The individuals described in this subsection are employees of elements of the intelligence community and the dependents or other immediate family members of such employees.

(Pub. L. 117–103, div. X, title VI, §604, Mar. 15, 2022, 136 Stat. 996.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 2 of div. X of Pub. L. 117–103, set out as a note under section 3003 of this title.

§ 3334k. Report on protocols for certain intelligence community employees and dependents

(a) In general

Beginning not later than 180 days after March 15, 2022, the President shall develop, for uniform implementation across the elements of the intelligence community, each of the protocols described in subsections (c) through (f). Such protocols shall be subject to review and revision on a periodic basis, and any implementation of such protocols shall be conducted in accordance with applicable laws and current clinical and professional practices of the interagency medical community.

(b) Privacy

No data collected pursuant to any protocol under this section may be used for research or analytical purposes without the written consent of the individual from whom such data was collected with respect to such use.

(c) Protocol on baseline medical testing

The protocol described in this subsection is a protocol for conducting voluntary baseline medical testing of covered employees, covered individuals, and the dependents of covered employees who are included on the overseas travel orders of the covered employee. Such protocol shall set forth the required elements of such baseline medical testing, such as—

- (1) standard lab collection and testing of relevant biofluids;
- (2) the conduct of relevant visual and auditory examinations;
- (3) the conduct of Acquired Brain Injury Tool assessments, or other relevant assessments for balance, eye motion, and cognition;

(4) the assessment of relevant medical histories; and

(5) the conduct of any other standard relevant medical or neurological examinations, testing, or assessments.

(d) Protocols on post-incident medical testing

The protocols described in this subsection are protocols to enable voluntary medical testing and the coordination of treatment for covered employees, covered individuals, and the dependents of covered employees, following a reported anomalous health incident, such as—

(1) a protocol that sets forth elements, similar to the elements described in subsection (c), of such testing;

(2) a protocol pertaining to the voluntary testing and treatment for victims of anomalous health incidents who are children;

(3) a protocol for ensuring that all victims of anomalous health incidents receive access to prompt and consistent medical treatment, including from medical professionals holding appropriate security clearances and medical professionals with expertise in child care;

(4) a protocol for ensuring that all victims of anomalous health incidents are offered options for psychological treatment for the effects of such incidents; and

(5) a protocol for ensuring that any testing, evaluation, or collection of biofluids or other samples following a reported anomalous health incident may be compared against the baseline for the victim of the anomalous health incident, to the extent the individual participated in the baseline medical testing, consistent with subsections (b) and (c).

(e) Protocol on information collection, storage, and safeguarding

The protocol described in this subsection is a protocol for the collection, storage, and safeguarding of information acquired as a result of the protocols described in subsections (c) and (d).

(f) Protocol on reporting mechanisms

The protocol described in this subsection is a protocol for the reporting of matters relating to anomalous health incidents by covered employees, covered individuals, and the dependents of covered employees, including the development of a system for the adjudication of complaints regarding medical treatment received by such covered employees, covered individuals, and dependents of covered employees.

(g) Report and briefings

(1) Report

Not later than 180 days after March 15, 2022, the Director of National Intelligence shall submit to the appropriate congressional committees a report on the protocols described in subsections (c) through (f).

(2) Elements

Such report shall include the following elements:

(A) A copy of each protocol under this section.

(B) A description of the following:

(i) Any interagency agreements, authorities, or policies required to effectively implement the protocols under this section.

(ii) Any new facilities, medical equipment, tools, training, or other resources required to effectively implement such protocols.

(C) A timeline for the implementation of the protocols under this section, including a proposal for the prioritization of implementation with respect to various categories of covered employees and the dependents of covered employees.

(3) Briefing

Not later than 60 days following the date of submission of the report under paragraph (1), and biannually thereafter, the Director shall provide to the appropriate congressional committees a briefing regarding the implementation of the protocols under this section.

(h) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

(A) the congressional intelligence committees; and

(B) the Committees on Armed Services of the House of Representatives and the Senate.

(2) Covered employee

The term “covered employee” means an individual who is an employee, assignee, or detailee of an element of the intelligence community.

(3) Covered individual

The term “covered individual” means a contractor to an element of the intelligence community.

(4) Dependent of a covered employee

The term “dependent of a covered employee” means, with respect to a covered employee, a family member (including a child), as defined by the Director of National Intelligence.

(5) Victim of an anomalous health incident

The term “victim of an anomalous health incident” means a covered employee, covered individual, or dependent of a covered employee, who is, or is suspected to have been, affected by an anomalous health incident.

(Pub. L. 117–103, div. X, title VI, § 605, Mar. 15, 2022, 136 Stat. 996.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “congressional intelligence committees” and “intelligence community” as used in this section, see section 2 of div. X of Pub. L. 117–103, set out as a note under section 3003 of this title.

§ 3334I. Oversight of Defense Intelligence Agency culture

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term “appropriate committees of Congress” means—

(A) the congressional intelligence committees;

(B) the Committee on Armed Services of the Senate;

(C) the Subcommittee on Defense of the Committee on Appropriations of the Senate;

(D) the Committee on Armed Services of the House of Representatives; and

(E) the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

(2) Workforce climate survey

The term “workforce climate survey”—

(A) means a workforce engagement or climate survey conducted at the agency, directorate, career field, or integrated intelligence center level, without regard to whether the survey is conducted on an annual or ad-hoc basis; and

(B) does not include an exit survey specified in subsection (c).

(b) Findings

Congress finds that the Defense Intelligence Agency has committed to improving Agency culture and leadership; however, actions taken by the Agency as of December 23, 2022, have not enabled a full assessment of the extent of workforce culture issues and potential management abuses, and require additional congressional oversight to ensure concerns are both understood and addressed.

(c) Mandatory provision of exit survey or interview

(1) In general

The Director of the Defense Intelligence Agency shall ensure that each employee of such Agency who leaves employment with such Agency (but not including any detail assignment) completes an exit survey or exit interview prior to such departure, to the extent practicable.

(2) Annual submissions to Congress

On an annual basis during the 3-year period beginning on December 23, 2022, the Director of the Defense Intelligence Agency shall submit to the appropriate committees of Congress a written analysis of the results of the exit surveys or exit interviews completed pursuant to paragraph (1) during the year covered by the report together with a plan of the Director to address any issues identified pursuant to such results to improve retention and culture.

(d) Congressional oversight relating to workforce climate surveys

(1) Notifications of ad-hoc workforce climate surveys

Not later than 14 days after the date on which the Director of the Defense Intelligence Agency conducts an ad-hoc workforce climate survey (including in response to a specific incident or concern), the Director shall notify the appropriate committees of Congress.

(2) Reports on final results

Not later than 90 days after the date on which the Director of the Defense Intelligence Agency concludes the conduct of any work-

force climate survey, the Director shall submit to the appropriate committees of Congress a report containing the final results of such workforce climate survey. Such report shall include the following:

(A) The topic of the workforce climate survey, and the workforce level surveyed.

(B) The rationale for conducting the workforce climate survey.

(C) The measures in place to ensure the accessibility of the workforce climate survey.

(D) The lead official or entity conducting the workforce climate survey.

(E) Any actions the Director intends to take, or is considering, in response to the results of the workforce climate survey.

(3) Accessibility of workforce climate surveys

The Director of the Defense Intelligence Agency shall ensure that, to the extent practicable, and consistent with the protection of intelligence sources and methods, workforce climate surveys are accessible to employees of such Agency on classified and unclassified systems.

(e) Feasibility report

Not later than 270 days after December 23, 2022, the Director of the Defense Intelligence Agency shall submit to the appropriate committees of Congress a report containing an analysis of the feasibility (including the anticipated cost, personnel requirements, necessary authorities, and such other matters as may be determined appropriate by the Director for purposes of analyzing feasibility) of—

(1) conducting 360-degree performance reviews among employees of the Defense Intelligence Agency; and

(2) including leadership suitability assessments (including personality evaluations, communication style assessments, and emotional intelligence aptitude assessments) for promotions of such employees to a position within grade GS-14 or above of the General Schedule.

(Pub. L. 117–263, div. F, title LXIV, § 6422, Dec. 23, 2022, 136 Stat. 3530; Pub. L. 118–31, div. G, title IX, § 7901(b)(1), Dec. 22, 2023, 137 Stat. 1106.)

Editorial Notes

REFERENCES IN TEXT

The General Schedule, referred to in subsec. (e)(2), is set out under section 5332 of Title 5, Government Organization and Employees.

AMENDMENTS

2023—Subsec. (b). Pub. L. 118–31 substituted “congressional” for “Congressional”.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.

§ 3334m. Additional responsibilities of Director of National Intelligence for artificial intelligence policies, standards, and guidance for the intelligence community

(a) Responsibilities of Director of National Intelligence

The Director of National Intelligence, in consultation with the heads of the elements of the intelligence community or the officials designated under subsection (c), shall—

(1) establish, and periodically conduct reviews of, policies, standards, and procedures relating to the acquisition, adoption, development, use, coordination, and maintenance of artificial intelligence capabilities and associated data, frameworks, computing environments, and other enablers by the intelligence community (including by incorporating and updating such policies based on emerging technology capabilities), to accelerate and increase the adoption of artificial intelligence capabilities within the intelligence community;

(2) ensure policies established or updated pursuant to paragraph (1) are consistent with—

(A) the principles outlined in the guidance of the Office of the Director of National Intelligence titled “Principles of Artificial Intelligence Ethics for the Intelligence Community and its Artificial Intelligence Ethics Framework for the Intelligence Community”, or any successor guidance; and

(B) any other principles developed by the Director relating to the governance, documentation, auditability, or evaluation of artificial intelligence systems or the accurate, secure, ethical, and reliable adoption or use of artificial intelligence; and

(3) provide to the heads of the elements of the intelligence community guidance for developing the National Intelligence Program budget pertaining to such elements to facilitate the acquisition, adoption, development, use, and maintenance of element-specific artificial intelligence capabilities, and to ensure the associated data, frameworks, computing environments, and other enablers are appropriately prioritized.

(b) Policies

(1) In general

In carrying out subsection (a)(1), not later than 1 year after December 22, 2023, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, the Director of the Office of Management and Budget, and such other officials as the Director of National Intelligence determines appropriate, shall establish the policies described in paragraph (2).

(2) Policies described

The policies described in this paragraph are policies for the acquisition, adoption, development, use, coordination, and maintenance of artificial intelligence capabilities that—

(A) establish a lexicon relating to the use of machine learning and artificial intelligence developed or acquired by elements of the intelligence community;

(B) establish minimum guidelines for evaluating the performance of models developed or acquired by elements of the intelligence community, such as by—

(i) specifying conditions for the continuous monitoring of artificial intelligence capabilities for performance, including the conditions for retraining or retiring models based on performance;

(ii) documenting performance objectives, including specifying how performance objectives shall be developed and contractually enforced for capabilities procured from third parties;

(iii) specifying the manner in which models should be audited, as necessary, including the types of documentation that should be provided to any auditor; and

(iv) specifying conditions under which models used by elements of the intelligence community should be subject to testing and evaluation for vulnerabilities to techniques meant to undermine the availability, integrity, or privacy of an artificial intelligence capability;

(C) establish minimum guidelines for tracking dependencies in adjacent systems, capabilities, or processes impacted by the retraining or sunseting of any model described in subparagraph (B);

(D) establish minimum documentation requirements for capabilities procured from third parties, aligning such requirements, as necessary, with existing documentation requirements applicable to capabilities developed by elements of the intelligence community;

(E) establish minimum standards for the documentation of imputed, augmented, or synthetic data used to train any model developed, procured, or used by an element of the intelligence community; and

(F) provide guidance on the acquisition and usage of models that have previously been trained by a third party for subsequent modification and usage by such an element.

(3) Policy review and revision

The Director of National Intelligence shall annually review or revise each policy established under paragraph (1).

(c) Designated leads within each element of the intelligence community

Each head of an element of the intelligence community, in coordination with the Director of National Intelligence, shall identify a senior official within the element to serve as the designated element lead responsible for overseeing and coordinating efforts relating to artificial intelligence, including through the integration of the acquisition, technology, human capital, and financial management aspects necessary for the adoption of artificial intelligence solutions. Such designated element leads shall meet regularly to consult and coordinate with the Director of National Intelligence regarding the implementation of this section and this title.¹

¹ See References in Text note below.

(Pub. L. 117–263, div. F, title LXVII, § 6702, Dec. 23, 2022, 136 Stat. 3561; Pub. L. 118–31, div. G, title V, § 7513(a), Dec. 22, 2023, 137 Stat. 1095.)

Editorial Notes

REFERENCES IN TEXT

This title, referred to in subsec. (c), means title LXVII of div. F of Pub. L. 117–263, Dec. 23, 2022, 136 Stat. 3560, which enacted this section and sections 3034b, 3334n, and 3334o of this title, amended sections 3024 and 3030 of this title, and enacted provisions set out as notes under sections 3024 and 3030 of this title. For complete classification of title LXVII to the Code, see Tables.

AMENDMENTS

2023—Subsec. (a). Pub. L. 118–31, § 7513(a)(1), substituted “subsection (c)” for “subsection (b)” in introductory provisions.

Subsecs. (b), (c). Pub. L. 118–31, § 7513(a)(2), (3), added subsec. (b) and redesignated former subsec. (b) as (c).

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.

For definitions of “artificial intelligence” and “emerging technology” as used in this section, see section 6701 of Pub. L. 117–263, set out as a note under section 3024 of this title.

§ 3334n. Certification relating to information technology and software systems

(a) Certifications required

Prior to the date on which the head of an element of the intelligence community enters into, renews, or extends a contract for the acquisition of an information technology or software system, the head shall certify to the Director of National Intelligence the following:

(1) That the information technology or software system is the most up-to-date version of the system available or, if it is not, why a more out of date version was chosen.

(2) That the information technology or software system is compatible with integrating new and emerging technologies, such as artificial intelligence.

(3) That the information technology or software system was thoroughly reviewed and alternative products are not superior to meet the requirements of the element.

(b) Exemption

The Director of National Intelligence may exempt elements of the intelligence community, as appropriate, from the requirements under (a)¹ if meeting such requirements may pose security or operational risks.

(c) Guidance

The Director shall issue to the heads of the elements of the intelligence community, and submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives, guidance to—

¹ So in original. Probably should be “subsection (a)”.

(1) establish guidelines that the heads of the relevant elements of the intelligence community shall use to evaluate the criteria required for the certifications under subsection (a);

(2) incentivize each such head to adopt and integrate new and emerging technology within information technology and software systems of the element and to decommission and replace outdated systems, including through potential funding enhancements; and

(3) incentivize, and hold accountable, personnel of the intelligence community with respect to the integration of new and emerging technology within such systems, including through the provision of appropriate training programs and evaluations.

(Pub. L. 117–263, div. F, title LXVII, § 6718, Dec. 23, 2022, 136 Stat. 3577.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.

For definitions of “emerging technology” and “artificial intelligence” as used in this section, see section 6701 of Pub. L. 117–263, set out as a note under section 3024 of this title.

§ 3334o. Requirements and report on workforce needs of intelligence community relating to science, technology, engineering, and math, and related areas

(a) Requirements

The Director of National Intelligence, in coordination with the heads of human capital from each element of the intelligence community, shall—

(1) develop a plan for the recruitment and retention of personnel to positions the primary duties of which involve the integration, maintenance, or use of artificial intelligence (and the retention and training of personnel serving in such positions), including with respect to the authorities and requirements under section 6732(b);¹

(2) develop a plan for the review and evaluation, on a continuous basis, of the expertise necessary to accelerate the adoption of artificial intelligence and other emerging technology solutions; and

(3) coordinate and share information and best practices relating to such recruitment and retention within the element and across the intelligence community.

(b) Report

(1) Submission

Not later than January 1, 2024, the Director of National Intelligence, in coordination with heads of human capital from each element of the intelligence community, shall submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representa-

tives a single report on the workforce needs of each element of the intelligence community relating to emerging technologies, with a specific focus on artificial intelligence.

(2) Elements

The report under paragraph (1) shall include, with respect to each element of the intelligence community, the following:

(A) A description of the number and types of personnel in work roles whose primary official duties include artificial intelligence responsibilities.

(B) A detailed description of the plans for each element developed pursuant to subsection (a).

(3) Other matters

The report under paragraph (1) shall also include an assessment of the quality and sustainability of the talent pipeline of the intelligence community with respect to talent in emerging technologies, including artificial intelligence. Such assessment shall include the following:

(A) A description of the education, recruitment, and retention programs (including skills-based training and career and technical educational programs) available to personnel of the intelligence community, regardless of whether such programs are administered by the head of an element of the intelligence community or the head of another Federal department or agency, and an analysis of how such programs support the quality and sustainability of such talent pipeline.

(B) A description of the relevant authorities available to the heads of the elements of the intelligence community to promote the quality and sustainability of such talent pipeline.

(C) An assessment of any gaps in authorities, resources, recruitment or retention incentives, skills-based training, or educational programs, that may negatively affect the quality or sustainability of such talent pipeline.

(4) Form

The report under paragraph (1) shall be submitted in classified or unclassified form, as appropriate.

(c) Information access

The heads of the elements of the intelligence community shall furnish to the Director of National Intelligence such information as may be necessary for the development of the report under subsection (b).

(Pub. L. 117–263, div. F, title LXVII, § 6723, Dec. 23, 2022, 136 Stat. 3581.)

Editorial Notes

REFERENCES IN TEXT

Section 6732(b), referred to in subsec. (a)(1), means section 6732(b) of Pub. L. 117–263, which is set out in a note under section 3024 of this title.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in

¹ See References in Text note below.

this section, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.

For definitions of “artificial intelligence” and “emerging technology” as used in this section, see section 6701 of Pub. L. 117–263, set out as a note under section 3024 of this title.

§ 3334p. Increased intelligence-related engineering, research, and development capabilities of minority institutions

(a) Plan

(1) Requirement

The Director of National Intelligence shall develop a plan to promote intelligence-related engineering, research, and development activities at covered institutions for the purpose of contributing toward the research necessary to achieve the intelligence advantage of the United States.

(2) Elements

The plan under paragraph (1) shall include the following:

(A) An assessment of opportunities to support engineering, research, and development at covered institutions in computer sciences, including artificial intelligence, quantum computing, and machine learning, and synthetic biology and an assessment of opportunities to support the associated workforce and physical research infrastructure of such institutions.

(B) An assessment of opportunities to enhance the ability of covered institutions—

(i) to participate in intelligence-related engineering, research, and development activities; and

(ii) to effectively compete for intelligence-related engineering, research and development contracts in support of the most urgent research requirements of the intelligence community.

(C) An assessment of the activities and investments the Director determines necessary—

(i) to expand opportunities for covered institutions to partner with other research organizations and educational institutions that the intelligence community frequently partners with to conduct research; and

(ii) to increase participation of covered institutions in intelligence-related engineering, research, and development activities.

(D) Recommendations identifying actions that may be taken by the Director, Congress, covered institutions, and other organizations to increase participation of such institutions in intelligence-related engineering, research, and development activities and contracts.

(E) Specific goals, incentives, and metrics to increase and measure the capacity of covered institutions to address the engineering, research, and development needs of the intelligence community.

(3) Consultation

In developing the plan under paragraph (1), the Director shall consult with covered insti-

tutions and other departments or agencies of the United States Government or private sector organizations that the Director determines appropriate.

(4) Report

Not later than 1 year after December 23, 2022, the Director shall submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives, and make publicly available on the internet website of the Director, a report containing the plan under paragraph (1).

(b) Activities to support research and engineering capacity

Subject to the availability of appropriations for such purpose, the Director may establish a program to award contracts, grants, or other agreements, on a competitive basis, and to perform other appropriate activities, for any of the following purposes:

(1) Developing the capability, including the workforce and the research infrastructure, for covered institutions to more effectively compete for intelligence-related engineering, research, and development activities and contracts.

(2) Any other purposes the Director determines appropriate to enhance the capabilities of covered institutions to carry out intelligence-related engineering, research, and development activities and contracts.

(c) Increased partnerships between IARPA and covered institutions

The Director shall establish goals and incentives to encourage the Intelligence Advanced Research Projects Activity to—

(1) partner with covered institutions to advance the research and development needs of the intelligence community through partnerships and collaborations with the Intelligence Advanced Research Projects Activity; and

(2) if the Director determines appropriate, foster the establishment of similar relationships between such institutions and other organizations that have partnerships with the Intelligence Advanced Research Projects Activity.

(d) Covered institution defined

In this section, the term “covered institution” means the following:

(1) A part B institution (as defined in section 1061 of title 20).

(2) An institution of higher education (as defined in section 1001 of title 20) not covered by paragraph (1) at which not less than 50 percent of the total student enrollment consists of students from ethnic groups that are underrepresented in the fields of science and engineering, as determined by the Director of National Intelligence.

(Pub. L. 117–263, div. F, title LXVIII, § 6812, Dec. 23, 2022, 136 Stat. 3602.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 6002 of Pub. L. 117-263, set out as a note under section 3003 of this title.

§ 3334q. Detail of individuals from intelligence community to Department of Commerce**(a) Authority**

In order to better facilitate the sharing of actionable intelligence on foreign adversary intent, capabilities, threats, and operations that pose a threat to the interests or security of the United States, particularly as they relate to the procurement, development, and use of dual-use and emerging technologies, the Director of National Intelligence may, acting through the Intelligence Community Civilian Joint Duty Program and in consultation with the Secretary of Commerce, advertise joint duty positions and detail or facilitate the detail of civilian employees from across the intelligence community to the Bureau of Industry and Security of the Department of Commerce.

(b) Detail

Detailees on a joint duty assignment (JDA) assigned pursuant to subsection (a) shall be drawn from such elements of the intelligence community as the Director considers appropriate, in consultation with the Secretary of Commerce.

(c) Expertise

The Director shall ensure that detailees referred to in subsection (a) have subject matter expertise on countries of concern, including China, Iran, North Korea, and Russia, as well as functional areas such as illicit procurement, counterproliferation, emerging and foundational technology, economic and financial intelligence, information and communications technology systems, supply chain vulnerability, and counterintelligence.

(d) Duty credit

The detail of an employee of the intelligence community to the Department of Commerce under subsection (a) shall be without interruption or loss of civil service status or privilege.

(Pub. L. 118-31, div. G, title V, §7501, Dec. 22, 2023, 137 Stat. 1079.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 7002 of Pub. L. 118-31, set out as a note under section 3003 of this title.

§ 3334r. Designation of a chief technology officer within certain elements of the intelligence community**(a) Designation authority**

The head of each covered element of the intelligence community shall designate a senior official to serve as the chief technology officer of such element.

(b) Covered elements

For purposes of this section, the covered elements of the intelligence community are the following:

- (1) The Central Intelligence Agency.
- (2) The Defense Intelligence Agency.
- (3) The Federal Bureau of Investigation.
- (4) The National Geospatial-Intelligence Agency.
- (5) The National Security Agency.
- (6) The National Reconnaissance Office.

(c) Responsibility

The chief technology officer of each covered element of the intelligence community shall be responsible for assisting the head of such element in the identification and adoption of technology to advance mission needs.

(d) Prohibition of dual appointment

Any chief technology officer designated pursuant to subsection (a) may not concurrently serve as the chief information officer, the chief data officer, or the principal science officer of any element of the intelligence community.

(Pub. L. 118-31, div. G, title V, §7504, Dec. 22, 2023, 137 Stat. 1083.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 7002 of Pub. L. 118-31, set out as a note under section 3003 of this title.

§ 3334s. Programs for next-generation microelectronics in support of artificial intelligence**(a) Program establishment**

Subject to the availability of appropriations, the Director of National Intelligence, acting through the Director of the Intelligence Advanced Research Projects Activity, shall establish or otherwise oversee a program to advance microelectronics research.

(b) Research focus

The Director of National Intelligence shall ensure that the research carried out under the program established under subsection (a) is focused on the following:

- (1) Advanced engineering and applied research into next-generation computing models, materials, devices, architectures, and algorithms to enable the advancement of artificial intelligence and machine learning.
- (2) Efforts to—

(A) overcome challenges with engineering and applied research of microelectronics, including with respect to the physical limits on transistors, electrical interconnects, and memory elements;¹

(B) promote long-term advancements in computing technologies, including by fostering a unified and multidisciplinary approach encompassing research and development into—

- (i) next-generation algorithm design;
- (ii) next-generation compute capability;
- (iii) generative and adaptive artificial intelligence for design applications;
- (iv) photonics-based microprocessors, including electrophotonics;
- (v) the chemistry and physics of new materials;

¹ So in original. Probably should be followed by “and”.

- (vi) optical communication networks, including electrophotonics; and
- (vii) safety and controls for generative artificial intelligence applications for the intelligence community.

(3) Any other activity the Director determines would promote the development of microelectronics research for future technologies, including optical communications or quantum technologies.

(c) Consideration, consultation, and collaboration

In carrying out the program established under subsection (a), the Director of National Intelligence shall—

- (1) consider the national strategy developed pursuant to subsection (a)(3)(A)(i) of section 4656 of title 15;
- (2) consult with the Secretary of Commerce; and
- (3) actively collaborate with relevant Government agencies and programs, including the programs established under subsection² (c), (d), (e), and (f) of such section 4656 of title 15, academic institutions, and private industry to leverage expertise and resources in conducting research.

(d) Authorization of appropriations

Amounts authorized to be appropriated for the National Intelligence Program of the Office of the Director of National Intelligence may be made available to carry out the program established under subsection (a).

(e) Briefing requirements

The Director of the Intelligence Advanced Research Projects Activity shall provide to the congressional intelligence committees, the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and, consistent with the protection of intelligence sources and methods, the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives, regular briefings on—

- (1) the progress, achievements, and outcomes of the program established under subsection (a);
- (2) the collaborations conducted pursuant to subsection (c); and
- (3) recommendations for future research priorities.

(Pub. L. 118–31, div. G, title V, § 7507, Dec. 22, 2023, 137 Stat. 1089.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.

§ 3334t. Program for beyond 5G

(a) Establishment

The Director of National Intelligence, acting through the Director of the Intelligence Ad-

vanced Research Projects Activity, may initiate or otherwise carry out a program dedicated to research and development efforts relevant to 6G technology and any successor technologies, but only if such efforts are specific to potential applications of 6G technology (or any successor technologies) for the intelligence community or for other national security purposes.

(b) Consultation and coordination

In carrying out any program under subsection (a), the Director shall consult and coordinate with—

- (1) relevant—

(A) heads of Federal departments and agencies, including the Administrator of the National Telecommunications and Information Administration;

(B) interagency bodies, such as the Committee for the Assessment of Foreign Participation in the United States Telecommunications Sector;

(C) private sector entities;

(D) institutions of higher learning; and

(E) federally funded research and development centers; and

- (2) such other individuals and entities as the Director determines appropriate.

(c) 6G technology defined

In this section, the term “6G technology” means hardware, software, or other technologies relating to sixth-generation wireless networks.

(Pub. L. 118–31, div. G, title V, § 7508, Dec. 22, 2023, 137 Stat. 1090.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.

§ 3334u. Notification of referral to Department of Justice

If a referral is made to the Department of Justice from any element of the intelligence community regarding an allegation of misconduct against a civilian employee of the intelligence community, the head of the element of the intelligence community that employs the covered employee shall notify the congressional intelligence committees of the referral not later than 10 days after the date on which such referral is made.

(Pub. L. 118–159, div. F, title LXVI, § 6614(c), Dec. 23, 2024, 138 Stat. 2506.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 6002 of div. F of Pub. L. 118–159, set out as a note under section 3003 of this title.

SUBCHAPTER III—SECURITY CLEARANCES AND CLASSIFIED INFORMATION

§ 3341. Security clearances

(a) Definitions

In this section:

² So in original. Probably should be “subsections”.

(1) The term “agency” means—

(A) an executive agency (as that term is defined in section 105 of title 5);

(B) a military department (as that term is defined in section 102 of title 5); or

(C) an element of the intelligence community.

(2) The term “authorized investigative agency” means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(3) The term “authorized adjudicative agency” means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term “highly sensitive program” means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 2014(y) of title 42); or

(ii) other information commonly referred to as “sensitive compartmented information”.

(5) The term “current investigation file” means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

(A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;

(B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance; and

(C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.

(6) The term “personnel security investigation” means any investigation required for the purpose of determining the eligibility of any military, civilian, or government contractor personnel to access classified information.

(7) The term “periodic reinvestigations” means investigations conducted for the purpose of updating a previously completed background investigation—

(A) every 5 years in the case of a top secret clearance or access to a highly sensitive program;

(B) every 10 years in the case of a secret clearance; or

(C) every 15 years in the case of a Confidential Clearance.

(8) The term “appropriate committees of Congress” means—

(A) the Permanent Select Committee on Intelligence and the Committees on Armed

Services, Homeland Security, Government Reform, and the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence and the Committees on Armed Services, Homeland Security and Governmental Affairs, and the Judiciary of the Senate.

(9) ACCESS DETERMINATION.—The term “access determination” means the determination regarding whether an employee—

(A) is eligible for access to classified information in accordance with Executive Order 12968 (60 Fed. Reg. 40245; relating to access to classified information), or any successor thereto, and Executive Order 10865 (25 Fed. Reg. 1583; relating to safeguarding classified information within industry), or any successor thereto; and

(B) possesses a need to know under such an Order.

(b) Selection of entity

Except as otherwise provided, not later than 90 days after December 17, 2004, the President shall select a single department, agency, or element of the executive branch to be responsible for—

(1) directing day-to-day oversight of investigations and adjudications for personnel security clearances, including for highly sensitive programs, throughout the United States Government;

(2) developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures;

(3) serving as the final authority to designate an authorized investigative agency or authorized adjudicative agency;

(4) ensuring reciprocal recognition of access to classified information among the agencies of the United States Government, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of security clearances and access to highly sensitive programs pursuant to subsection (d);

(5) ensuring, to the maximum extent practicable, that sufficient resources are available in each agency to achieve clearance and investigative program goals;

(6) reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and granting of clearances; and

(7) not later than 180 days after July 7, 2014, and consistent with subsection (j)—

(A) developing policies and procedures that permit, to the extent practicable, individuals alleging reprisal for having made a protected disclosure (provided the individual does not disclose classified information or other information contrary to law) to appeal any action affecting an employee’s access to classified information and to retain their government employment status while such challenge is pending; and

(B) developing and implementing uniform and consistent policies and procedures to en-

sure proper protections during the process for denying, suspending, or revoking a security clearance or access to classified information following a protected disclosure, including the ability to appeal such a denial, suspension, or revocation, except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts no longer than 1 year or the head of the agency or a designee of the head of the agency certifies that a longer suspension is needed before a final decision on denial or revocation to prevent imminent harm to the national security.

(c) Performance of security clearance investigations

(1) Notwithstanding any other provision of law, not later than 180 days after December 17, 2004, the President shall, in consultation with the head of the entity selected pursuant to subsection (b), select a single agency of the executive branch to conduct, to the maximum extent practicable, security clearance investigations of employees and contractor personnel of the United States Government who require access to classified information and to provide and maintain all security clearances of such employees and contractor personnel. The head of the entity selected pursuant to subsection (b) may designate other agencies to conduct such investigations if the head of the entity selected pursuant to subsection (b) considers it appropriate for national security and efficiency purposes.

(2) The agency selected under paragraph (1) shall—

(A) take all necessary actions to carry out the requirements of this section, including entering into a memorandum of understanding with any agency carrying out responsibilities relating to security clearances or security clearance investigations before December 17, 2004;

(B) as soon as practicable, integrate reporting of security clearance applications, security clearance investigations, and determinations of eligibility for security clearances, with the database required by subsection (e); and

(C) ensure that security clearance investigations are conducted in accordance with uniform standards and requirements established under subsection (b), including uniform security questionnaires and financial disclosure requirements.

(d) Reciprocity of security clearance and access determinations

(1) All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies.

(2) All security clearance background investigations initiated by an authorized investigative agency shall be transferable to any other authorized investigative agency.

(3)(A) An authorized investigative agency or authorized adjudicative agency may not establish additional investigative or adjudicative requirements (other than requirements for the

conduct of a polygraph examination) that exceed requirements specified in Executive Orders establishing security requirements for access to classified information without the approval of the head of the entity selected pursuant to subsection (b).

(B) Notwithstanding subparagraph (A), the head of the entity selected pursuant to subsection (b) may establish such additional requirements as the head of such entity considers necessary for national security purposes.

(4) An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual where a current investigation or clearance of equal level already exists or has been granted by another authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may disallow the reciprocal recognition of an individual security clearance by an agency under this section on a case-by-case basis if the head of the entity selected pursuant to subsection (b) determines that such action is necessary for national security purposes.

(6) The head of the entity selected pursuant to subsection (b) shall establish a review procedure by which agencies can seek review of actions required under this section.

(e) Database on security clearances

(1) Not later than 12 months after December 17, 2004, the Director of the Office of Personnel Management shall, in cooperation with the heads of the entities selected pursuant to subsections (b) and (c), establish and commence operating and maintaining an integrated, secure, database into which appropriate data relevant to the granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.

(2) The database under this subsection shall function to integrate information from existing Federal clearance tracking systems from other authorized investigative and adjudicative agencies into a single consolidated database.

(3) Each authorized investigative or adjudicative agency shall check the database under this subsection to determine whether an individual the agency has identified as requiring a security clearance has already been granted or denied a security clearance, or has had a security clearance revoked, by any other authorized investigative or adjudicative agency.

(4) The head of the entity selected pursuant to subsection (b) shall evaluate the extent to which an agency is submitting information to, and requesting information from, the database under this subsection as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may authorize an agency to withhold information about certain individuals from the database under this subsection if the head of the entity considers it necessary for national security purposes.

(f) Evaluation of use of available technology in clearance investigations and adjudications

(1) The head of the entity selected pursuant to subsection (b) shall evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for a security clearance.

(2) The evaluation shall assess the application of the technologies described in paragraph (1) for—

(A) granting interim clearances to applicants at the secret, top secret, and special access program levels before the completion of the appropriate full investigation;

(B) expediting investigations and adjudications of security clearances, including verification of information submitted by the applicant;

(C) ongoing verification of suitability of personnel with security clearances in effect for continued access to classified information;

(D) use of such technologies to augment periodic reinvestigations;

(E) assessing the impact of the use of such technologies on the rights of applicants to verify, correct, or challenge information obtained through such technologies; and

(F) such other purposes as the head of the entity selected pursuant to subsection (b) considers appropriate.

(3) An individual subject to verification utilizing the technology described in paragraph (1) shall be notified of such verification, shall provide consent to such use, and shall have access to data being verified in order to correct errors or challenge information the individual believes is incorrect.

(4) Not later than one year after December 17, 2004, the head of the entity selected pursuant to subsection (b) shall submit to the President and the appropriate committees of Congress a report on the results of the evaluation, including recommendations on the use of technologies described in paragraph (1).

(g), (h). Repealed. Pub. L. 118-31, div. G, title VII, §§ 7702(a)(3), 7703(c), Dec. 22, 2023, 137 Stat. 1101, 1102

(i) Authorization of appropriations

There is authorized to be appropriated such sums as may be necessary for fiscal year 2005 and each fiscal year thereafter for the implementation, maintenance, and operation of the database required by subsection (e).

(j) Retaliatory revocation of security clearances and access determinations

(1) In general

Agency personnel with authority to take, direct others to take, recommend, or approve personnel security clearance or access determinations shall not take or fail to take, or threaten to take or fail to take, any action with respect to any employee's security clearance or access determination in retaliation for—

(A) any lawful disclosure of information to the Director of National Intelligence (or an

employee designated by the Director of National Intelligence for such purpose) or a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including the head of the employing agency (or employee designated by the head of that agency for such purpose) by an employee that the employee reasonably believes evidences—

(i) a violation of any Federal law, rule, or regulation; or

(ii) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(B) any lawful disclosure to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee reasonably believes evidences—

(i) a violation of any Federal law, rule, or regulation; or

(ii) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(C) any lawful disclosure that complies with—

(i) subsections (a)(1), (d), and (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);¹

(ii) subparagraphs (A), (D), and (H) of section 3517(d)(5) of this title; or

(iii) subparagraphs (A), (D), and (I) of section 3033(k)(5) of this title; and

(D) if the actions do not result in the employee or applicant unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or

(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

(2) Rule of construction

Consistent with the protection of sources and methods, nothing in paragraph (1) shall be construed to authorize the withholding of information from Congress or the taking of any personnel action or clearance action against an employee who lawfully discloses information to Congress.

(3) Disclosures

A disclosure shall not be excluded from paragraph (1) because—

¹ See References in Text note below.

(A) the disclosure was made to a person, including a supervisor, who participated in an activity that the employee reasonably believed to be covered by paragraph (1)(A)(ii);

(B) the disclosure revealed information that had been previously disclosed;

(C) the disclosure was not made in writing;

(D) the disclosure was made while the employee was off duty;

(E) of the amount of time which has passed since the occurrence of the events described in the disclosure; or

(F) the disclosure was made during the normal course of duties of an employee.

(4) Agency adjudication

(A) Remedial procedure

An employee or former employee who believes that he or she has been subjected to a reprisal prohibited by paragraph (1) may, within 90 days (except as provided by subparagraph (D)) after the issuance of notice of such decision, appeal that decision within the agency of that employee or former employee through proceedings authorized by subsection (b)(7), except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts not longer than 1 year (or a longer period in accordance with a certification made under subsection (b)(7)).

(B) Corrective action

If, in the course of proceedings authorized under subparagraph (A), it is determined that the adverse security clearance or access determination violated paragraph (1), the agency shall take specific corrective action to return the employee or former employee, as nearly as practicable and reasonable, to the position such employee or former employee would have held had the violation not occurred. Such corrective action may include back pay and related benefits, travel expenses, and compensatory damages not to exceed \$300,000.

(C) Contributing factor

In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual, unless the agency demonstrates by a preponderance of the evidence that it would have taken the same action in the absence of such disclosure, giving the utmost deference to the agency's assessment of the particular threat to the national security interests of the United States in the instant matter.

(D) Tolling

The time requirement established by subparagraph (A) for an employee or former employee to appeal the decision of an agency may be tolled if the employee or former employee presents substantial credible evidence showing why the employee or former em-

ployee did not timely initiate the appeal and why the enforcement of the time requirement would be unfair, such as evidence showing that the employee or former employee—

(i) did not receive notice of the decision; or

(ii) could not timely initiate the appeal because of factors beyond the control of the employee or former employee.

(5) Appellate review of security clearance access determinations by Director of National Intelligence

(A) Appeal

Within 60 days after receiving notice of an adverse final agency determination under a proceeding under paragraph (4), an employee or former employee may appeal that determination in accordance with the procedures established under subparagraph (B).

(B) Policies and procedures

The Director of National Intelligence, in consultation with the Attorney General and the Secretary of Defense, shall develop and implement policies and procedures for adjudicating the appeals authorized by subparagraph (A).

(C) Congressional notification

Consistent with the protection of sources and methods, at the time the Director of National Intelligence issues an order regarding an appeal pursuant to the policies and procedures established by this paragraph, the Director of National Intelligence shall notify the congressional intelligence committees.

(6) Judicial review

Nothing in this section shall be construed to permit or require judicial review of any—

(A) agency action under this section; or

(B) action of the appellate review procedures established under paragraph (5).

(7) Private cause of action

Nothing in this section shall be construed to permit, authorize, or require a private cause of action to challenge the merits of a security clearance determination.

(8) Enforcement

Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5.

(9) Inclusion of contractor employees

In this subsection, the term “employee” includes an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of an agency. With respect to such employees, the term “employing agency” shall be deemed to be the contracting agency.

(Pub. L. 108-458, title III, § 3001, Dec. 17, 2004, 118 Stat. 3705; Pub. L. 113-126, title VI, § 602(a)(1), (b), (c), July 7, 2014, 128 Stat. 1416, 1417, 1419; Pub. L. 113-293, title III, § 310, Dec. 19, 2014, 128 Stat. 3999; Pub. L. 115-118, title I, § 110(c), Jan. 19, 2018, 132 Stat. 17; Pub. L. 117-103, div. X, title V,

“(a) **POLICY REQUIRED.**—Not later than 180 days after the date of the enactment of this Act [Mar. 15, 2022], the Director of National Intelligence shall issue a policy for measuring the total time it takes to transfer personnel with security clearances and eligibility for access to information commonly referred to as ‘sensitive compartmented information’ from one element of the intelligence community to another, or from one contract to another in the case of a contractor.

“(b) **REQUIREMENTS.**—The policy issued under subsection (a) shall—

“(1) to the degree practicable, cover all personnel who are moving to positions that require a security clearance and access to sensitive compartmented information;

“(2) cover the period from the first time an element of the intelligence community or company submits a request to an element of the intelligence community for the transfer of the employment of an individual with a clearance access or eligibility determination to another element of the intelligence community, to the time the individual is authorized by that receiving element to start to work in the new position; and

“(3) include analysis of all appropriate phases of the process, including polygraph, suitability determination, fitness determination, human resources review, transfer of the sensitive compartmented information access, and contract actions.

“(c) **UPDATED POLICIES.**—

“(1) **MODIFICATIONS.**—Not later than 1 year after the date on which the Director issues the policy under subsection (a), the Director shall issue modifications to such policies as the Director determines were issued before the issuance of the policy under such subsection and are relevant to such updated policy, as the Director considers appropriate.

“(2) **RECOMMENDATIONS.**—Not later than 1 year after the date on which the Director issues the policy under subsection (a), the Director shall submit to the appropriate congressional committees recommendations for legislative action to update metrics specified elsewhere in statute to measure parts of the process that support transfers described in subsection (a).

“(d) **ANNUAL REPORTS.**—Not later than 180 days after issuing the policy required by subsection (a) and not less frequently than once each year thereafter until the date that is 3 years after the date of such issuance, the Director shall submit to the appropriate congressional committees a report on the implementation of such policy. Such report shall address performance by department or agency and by clearance type in meeting such policy.

“(e) **APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.**—In this section, the term ‘appropriate congressional committees’ means—

“(1) the congressional intelligence committees; and

“(2) the Subcommittees on Commerce, Justice, Science, and Related Agencies of the Committees on Appropriations of the House of Representatives and the Senate.”

[For definitions of “congressional intelligence committees” and “intelligence community” as used in section 311 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.]

REQUIRED ELEMENTS OF POLICIES AND PROCEDURES

Pub. L. 113–126, title VI, §602(a)(2), July 7, 2014, 128 Stat. 1416, provided that: “The policies and procedures for appeal developed under paragraph (7) of section 3001(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 [50 U.S.C. 3341(b)(7)], as added by subsection (a), shall provide for the Inspector General of the Intelligence Community, or the inspector general of the employing agency, to conduct fact-finding and report to the agency head or the designee of the agency head within 180 days unless the employee and the agency agree to an extension or the investigating inspector general determines in writing that a greater

period of time is required. To the fullest extent possible, such fact-finding shall include an opportunity for the employee to present relevant evidence such as witness testimony.”

EXISTING RIGHTS PRESERVED

Pub. L. 113–126, title VI, §602(d), July 7, 2014, 128 Stat. 1419, provided that: “Nothing in this section [amending this section and enacting provisions set out as notes under this section] or the amendments made by this section shall be construed to preempt, preclude, or otherwise prevent an individual from exercising rights, remedies, or avenues of redress currently provided under any other law, regulation, or rule.”

STRATEGY FOR SECURITY CLEARANCE RECIPROCITY

Pub. L. 112–277, title III, §306, Jan. 14, 2013, 126 Stat. 2472, provided that:

“(a) **STRATEGY.**—The President shall develop a strategy and a schedule for carrying out the requirements of section 3001(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 435b(d)) [now 50 U.S.C. 3341(d)]. Such strategy and schedule shall include—

“(1) a process for accomplishing the reciprocity required under such section for a security clearance issued by a department or agency of the Federal Government, including reciprocity for security clearances that are issued to both persons who are and who are not employees of the Federal Government; and

“(2) a description of the specific circumstances under which a department or agency of the Federal Government may not recognize a security clearance issued by another department or agency of the Federal Government.

“(b) **CONGRESSIONAL NOTIFICATION.**—Not later than 180 days after the date of the enactment of this Act [Jan. 14, 2013], the President shall inform Congress of the strategy and schedule developed under subsection (a).”

§ 3342. Security clearances for transition team members

(1) Definition

In this section, the term “eligible candidate” has the meaning given such term by section 3(h)(4) of the Presidential Transition Act of 1963 (3 U.S.C. 102 note).

(2) In general

Each eligible candidate for President may submit, before the date of the general election, requests for security clearances for prospective transition team members who will have a need for access to classified information to carry out their responsibilities as members of the President-elect’s transition team.

(3) Completion date

Necessary background investigations and eligibility determinations to permit appropriate prospective transition team members to have access to classified information shall be completed, to the fullest extent practicable, by the day after the date of the general election.

(Pub. L. 108–458, title VII, §7601(c), Dec. 17, 2004, 118 Stat. 3857; Pub. L. 111–283, §2(c)(1), Oct. 15, 2010, 124 Stat. 3048.)

Editorial Notes

REFERENCES IN TEXT

This section, referred to in par. (1), is section 7601 of Pub. L. 108–458. See Codification note below.

Section 3(h)(4) of the Presidential Transition Act of 1963, referred to in par. (1), is section 3(h)(4) of Pub. L.

88-277, which is set out in a note under section 102 of Title 3, The President.

CODIFICATION

Section was formerly classified as a note under section 435b of this title prior to editorial reclassification as this section.

Section is comprised of subsec. (c) of section 7601 of Pub. L. 108-458. Subsec. (a) of section 7601 amended provisions set out as a note under section 102 of Title 3, The President, subsec. (b) of section 7601 is not classified to the Code, and subsec. (d) of section 7601 is set out as a note under section 102 of Title 3.

AMENDMENTS

2010—Par. (1). Pub. L. 111-283, §2(c)(1)(A), added par. (1) and struck out former par. (1) which read as follows: “In this section, the term ‘major party’ shall have the meaning given under section 9002(6) of title 26.”

Par. (2). Pub. L. 111-283, §2(c)(1)(B), substituted “eligible candidate” for “major party candidate”.

§ 3343. Security clearances; limitations

(a) Definitions

In this section:

(1) Controlled substance

The term “controlled substance” has the meaning given that term in section 802 of title 21.

(2) Covered person

The term “covered person” means—

(A) an officer or employee of a Federal agency;

(B) a member of the Army, Navy, Air Force, or Marine Corps who is on active duty or is in an active status; and

(C) an officer or employee of a contractor of a Federal agency.

(3) Restricted Data

The term “Restricted Data” has the meaning given that term in section 2014 of title 42.

(4) Special access program

The term “special access program” has the meaning given that term in section 4.1 of Executive Order No. 12958 (60 Fed. Reg. 19825).

(b) Prohibition

After January 1, 2008, the head of a Federal agency may not grant or renew a security clearance for a covered person who is an unlawful user of a controlled substance or an addict (as defined in section 802(1) of title 21).

(c) Disqualification

(1) In general

After January 1, 2008, absent an express written waiver granted in accordance with paragraph (2), the head of a Federal agency may not grant or renew a security clearance described in paragraph (3) for a covered person who—

(A) has been convicted in any court of the United States of a crime, was sentenced to imprisonment for a term exceeding 1 year, and was incarcerated as a result of that sentence for not less than 1 year;

(B) has been discharged or dismissed from the Armed Forces under dishonorable conditions; or

(C) is mentally incompetent, as determined by an adjudicating authority, based

on an evaluation by a duly qualified mental health professional employed by, or acceptable to and approved by, the United States Government and in accordance with the adjudicative guidelines required by subsection (d).

(2) Waiver authority

In a meritorious case, an exception to the disqualification in this subsection may be authorized if there are mitigating factors. Any such waiver may be authorized only in accordance with—

(A) standards and procedures prescribed by, or under the authority of, an Executive order or other guidance issued by the President; or

(B) the adjudicative guidelines required by subsection (d).

(3) Covered security clearances

This subsection applies to security clearances that provide for access to—

(A) special access programs;

(B) Restricted Data; or

(C) any other information commonly referred to as “sensitive compartmented information”.

(4) Annual report

(A) Requirement for report

Not later than February 1 of each year, the head of a Federal agency shall submit a report to the appropriate committees of Congress if such agency employs or employed a person for whom a waiver was granted in accordance with paragraph (2) during the preceding year. Such annual report shall not reveal the identity of such person, but shall include for each waiver issued the disqualifying factor under paragraph (1) and the reasons for the waiver of the disqualifying factor.

(B) Definitions

In this paragraph:

(i) Appropriate committees of Congress

The term “appropriate committees of Congress” means, with respect to a report submitted under subparagraph (A) by the head of a Federal agency—

(I) the congressional defense committees;

(II) the congressional intelligence committees;

(III) the Committee on Homeland Security and Governmental Affairs of the Senate;

(IV) the Committee on Oversight and Government Reform of the House of Representatives; and

(V) each Committee of the Senate or the House of Representatives with oversight authority over such Federal agency.

(ii) Congressional defense committees

The term “congressional defense committees” has the meaning given that term in section 101(a)(16) of title 10.

(iii) Congressional intelligence committees

The term “congressional intelligence committees” has the meaning given that term in section 3003 of this title.

(d) Adjudicative guidelines**(1) Requirement to establish**

The President shall establish adjudicative guidelines for determining eligibility for access to classified information.

(2) Requirements related to mental health

The guidelines required by paragraph (1) shall—

(A) include procedures and standards under which a covered person is determined to be mentally incompetent and provide a means to appeal such a determination; and

(B) require that no negative inference concerning the standards in the guidelines may be raised solely on the basis of seeking mental health counseling.

(Pub. L. 108-458, title III, §3002, as added Pub. L. 110-181, div. A, title X, §1072(a), Jan. 28, 2008, 122 Stat. 328.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 12958, referred to in subsec. (a)(4), which was formerly set out as a note under section 435 (now section 3161) of this title, was revoked by Ex. Ord. No. 13526, §6.2(g), Dec. 29, 2009, 75 F.R. 731.

CODIFICATION

Section was formerly classified to section 435c of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

§ 3344. Classification training program**(a) In general**

The head of each Executive agency, in accordance with Executive Order 13526, shall require annual training for each employee who has original classification authority. For employees who perform derivative classification, or are responsible for analysis, dissemination, preparation, production, receipt, publication, or otherwise communication of classified information, training shall be provided at least every two years. Such training shall—

(1) educate the employee, as appropriate, regarding—

(A) the guidance established under subparagraph (G) of section 3024(g)(1) of this title, as added by section 5(a)(3),¹ regarding the formatting of finished intelligence products;

(B) the proper use of classification markings, including portion markings that indicate the classification of portions of information; and

(C) any incentives and penalties related to the proper classification of intelligence information; and

(2) ensure such training is a prerequisite, once completed successfully, as evidenced by an appropriate certificate or other record, for—

(A) obtaining original classification authority or derivatively classifying information; and

(B) maintaining such authority.

(b) Relationship to other programs

The head of each Executive agency shall ensure that the training required by subsection (a) is conducted efficiently and in conjunction with any other required security, intelligence, or other training programs to reduce the costs and administrative burdens associated with carrying out the training required by subsection (a).

(Pub. L. 111-258, §7, Oct. 7, 2010, 124 Stat. 2652.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13526, referred to in subsec. (a), is set out as a note under section 3161 of this title.

Section 5(a)(3), referred to in subsec. (a)(1)(A), probably means section 5(a)(3) of Pub. L. 111-258.

CODIFICATION

Section was formerly classified to section 435d of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries

DEFINITIONS

Pub. L. 111-258, §3, Oct. 7, 2010, 124 Stat. 2648, provided that: “In this Act [see Short Title of 2010 Amendment note set out under section 101 of Title 6, Domestic Security]:

“(1) DERIVATIVE CLASSIFICATION AND ORIGINAL CLASSIFICATION.—The terms ‘derivative classification’ and ‘original classification’ have the meanings given those terms in Executive Order No. 13526 [50 U.S.C. 3161 note].

“(2) EXECUTIVE AGENCY.—The term ‘Executive agency’ has the meaning given that term in section 105 of title 5, United States Code.

“(3) EXECUTIVE ORDER NO. 13526.—The term ‘Executive Order No. 13526’ means Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) or any subsequent corresponding executive order.”

§ 3344a. Training to promote sensible classification**(a) Definitions**

In this section:

(1) Over-classification

The term “over-classification” means classification at a level that exceeds the minimum level of classification that is sufficient to protect the national security of the United States.

(2) Sensible classification

The term “sensible classification” means classification at a level that is the minimum level of classification that is sufficient to protect the national security of the United States.

¹ See References in Text note below.

(b) Training required

Each head of an agency with classification authority shall conduct training for employees of the agency with classification authority to hold employees accountable for over-classification and to promote sensible classification.

(Pub. L. 118–31, div. G, title VI, §7603, Dec. 22, 2023, 137 Stat. 1097.)

§ 3345. Limitation on handling, retention, and storage of certain classified materials by the Department of State**(a) Certification regarding full compliance with requirements**

The Director of Central Intelligence shall certify to the appropriate committees of Congress whether or not each covered element of the Department of State is in full compliance with all applicable directives of the Director of Central Intelligence relating to the handling, retention, or storage of covered classified material.

(b) Limitation on certification

The Director of Central Intelligence may not certify a covered element of the Department of State as being in full compliance with the directives referred to in subsection (a) if the covered element is currently subject to a waiver of compliance with respect to any such directive.

(c) Report on noncompliance

Whenever the Director of Central Intelligence determines that a covered element of the Department of State is not in full compliance with any directive referred to in subsection (a), the Director shall promptly notify the appropriate committees of Congress of such determination.

(d) Effects of certification of non-full compliance

(1) Subject to subsection (e), effective as of January 1, 2001, a covered element of the Department of State may not retain or store covered classified material unless the Director has certified under subsection (a) as of such date that the covered element is in full compliance with the directives referred to in subsection (a).

(2) If the prohibition in paragraph (1) takes effect in accordance with that paragraph, the prohibition shall remain in effect until the date on which the Director certifies under subsection (a) that the covered element involved is in full compliance with the directives referred to in that subsection.

(e) Waiver by Director of Central Intelligence

(1) The Director of Central Intelligence may waive the applicability of the prohibition in subsection (d) to an element of the Department of State otherwise covered by such prohibition if the Director determines that the waiver is in the national security interests of the United States.

(2) The Director shall submit to appropriate committees of Congress a report on each exercise of the waiver authority in paragraph (1).

(3) Each report under paragraph (2) with respect to the exercise of authority under paragraph (1) shall set forth the following:

- (A) The covered element of the Department of State addressed by the waiver.
- (B) The reasons for the waiver.

(C) The actions that will be taken to bring such element into full compliance with the directives referred to in subsection (a), including a schedule for completion of such actions.

(D) The actions taken by the Director to protect any covered classified material to be handled, retained, or stored by such element pending achievement of full compliance of such element with such directives.

(f) Definitions

In this section:

(1) The term “appropriate committees of Congress” means the following:

(A) The Select Committee on Intelligence and the Committee on Foreign Relations of the Senate.

(B) The Permanent Select Committee on Intelligence and the Committee on International Relations of the House of Representatives.

(2) The term “covered classified material” means any material classified at the Sensitive Compartmented Information (SCI) level.

(3) The term “covered element of the Department of State” means each element of the Department of State that handles, retains, or stores covered classified material.

(4) The term “material” means any data, regardless of physical form or characteristic, including written or printed matter, automated information systems storage media, maps, charts, paintings, drawings, films, photographs, engravings, sketches, working notes, papers, reproductions of any such things by any means or process, and sound, voice, magnetic, or electronic recordings.

(5) The term “Sensitive Compartmented Information (SCI) level”, in the case of classified material, means a level of classification for information in such material concerning or derived from intelligence sources, methods, or analytical processes that requires such information to be handled within formal access control systems established by the Director of Central Intelligence.

(Pub. L. 106–567, title III, §309, Dec. 27, 2000, 114 Stat. 2840.)

Editorial Notes**CODIFICATION**

Section was formerly classified to section 435a of this title prior to editorial reclassification and renumbering as this section.

Statutory Notes and Related Subsidiaries**CHANGE OF NAME**

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of this title.

Committee on International Relations of House of Representatives changed to Committee on Foreign Af-

fairs of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

§ 3346. Compilation and organization of previously declassified records

(a), (b) Omitted

(c) Compilation and organization of records

The Department of Defense may not be required, when conducting a special search, to compile or organize records that have already been declassified and placed into the public domain.

(d) Special searches

For the purpose of this section, the term “special search” means the response of the Department of Defense to any of the following:

- (1) A statutory requirement to conduct a declassification review on a specified set of agency records.
- (2) An Executive order to conduct a declassification review on a specified set of agency records.
- (3) An order from the President or an official with delegated authority from the President to conduct a declassification review on a specified set of agency records.

(Pub. L. 106-398, § 1 [[div. A], title X, § 1075], Oct. 30, 2000, 114 Stat. 1654, 1654A-280.)

Editorial Notes

REFERENCES IN TEXT

This section, referred to in subsec. (d), is section 1075 of H.R. 5408 of the 106th Congress, as introduced on Oct. 6, 2000, and as enacted into law by section 1 of Pub. L. 106-398, Oct. 30, 2000, 114 Stat. 1654. See Codification note below.

CODIFICATION

Section was formerly classified as a note under section 435 of this title prior to editorial reclassification as this section.

Section is comprised of section 1075 of H.R. 5408 of the 106th Congress, as introduced on Oct. 6, 2000, and as enacted into law by section 1 of Pub. L. 106-398, Oct. 30, 2000, 114 Stat. 1654. Subsec. (a) of section 1075 amended former section 230 of Title 10, Armed Forces and subsec. (b) of section 1075 was not classified to the Code.

§ 3347. Secrecy agreements used in intelligence activities

Notwithstanding any other provision of law not specifically referencing this section, a non-disclosure policy form or agreement that is to be executed by a person connected with the conduct of an intelligence or intelligence-related activity, other than an employee or officer of the United States Government, may contain provisions appropriate to the particular activity for which such document is to be used. Such form or agreement shall, at a minimum—

- (1) require that the person will not disclose any classified information received in the course of such activity unless specifically authorized to do so by the United States Government; and
- (2) provide that the form or agreement does not bar—
 - (A) disclosures to Congress; or
 - (B) disclosures to an authorized official of an executive agency that are deemed essen-

tial to reporting a violation of United States law.

(Pub. L. 104-93, title III, § 306, Jan. 6, 1996, 109 Stat. 966.)

Editorial Notes

CODIFICATION

Section was formerly classified as a note under section 435 of this title prior to editorial reclassification as this section.

§ 3348. Reports relating to certain special access programs and similar programs

(a) In general

(1) Not later than February 1 of each year, the head of each covered department or agency shall submit to the congressional oversight committees a report on each special access program carried out in the department or agency.

(2) Each such report shall set forth—

(A) the total amount requested by the department or agency for special access programs within the budget submitted under section 1105 of title 31 for the fiscal year following the fiscal year in which the report is submitted; and

(B) for each program in such budget that is a special access program—

- (i) a brief description of the program;
- (ii) in the case of a procurement program, a brief discussion of the major milestones established for the program;
- (iii) the actual cost of the program for each fiscal year during which the program has been conducted before the fiscal year during which that budget is submitted; and
- (iv) the estimated total cost of the program and the estimated cost of the program for (I) the current fiscal year, (II) the fiscal year for which the budget is submitted, and (III) each of the four succeeding fiscal years during which the program is expected to be conducted.

(b) Newly designated programs

(1) Not later than February 1 of each year, the head of each covered department or agency shall submit to the congressional oversight committees a report that, with respect to each new special access program of that department or agency, provides—

- (A) notice of the designation of the program as a special access program; and
- (B) justification for such designation.

(2) A report under paragraph (1) with respect to a program shall include—

- (A) the current estimate of the total program cost for the program; and
- (B) an identification, as applicable, of existing programs or technologies that are similar to the technology, or that have a mission similar to the technology, or that have a mission similar to the mission, of the program that is the subject of the notice.

(3) In this subsection, the term “new special access program” means a special access program that has not previously been covered in a notice and justification under this subsection.

(c) Revision in classification of programs

(1) Whenever a change in the classification of a special access program of a covered depart-

ment or agency is planned to be made or whenever classified information concerning a special access program of a covered department or agency is to be declassified and made public, the head of the department or agency shall submit to the congressional oversight committees a report containing a description of the proposed change or the information to be declassified, the reasons for the proposed change or declassification, and notice of any public announcement planned to be made with respect to the proposed change or declassification.

(2) Except as provided in paragraph (3), a report referred to in paragraph (1) shall be submitted not less than 14 days before the date on which the proposed change, declassification, or public announcement is to occur.

(3) If the head of the department or agency determines that because of exceptional circumstances the requirement of paragraph (2) cannot be met with respect to a proposed change, declassification, or public announcement concerning a special access program of the department or agency, the head of the department or agency may submit the report required by paragraph (1) regarding the proposed change, declassification, or public announcement at any time before the proposed change, declassification, or public announcement is made and shall include in the report an explanation of the exceptional circumstances.

(d) Revision of criteria for designating programs

Whenever there is a modification or termination of the policy and criteria used for designating a program of a covered department or agency as a special access program, the head of the department or agency shall promptly notify the congressional oversight committees of such modification or termination. Any such notification shall contain the reasons for the modification or termination and, in the case of a modification, the provisions of the policy as modified.

(e) Waiver of reporting requirement

(1) The head of a covered department or agency may waive any requirement under subsection (a), (b), or (c) that certain information be included in a report under that subsection if the head of the department or agency determines that inclusion of that information in the report would adversely affect the national security. Any such waiver shall be made on a case-by-case basis.

(2) If the head of a department or agency exercises the authority provided under paragraph (1), the head of the department or agency shall provide the information described in that subsection with respect to the special access program concerned, and the justification for the waiver, to the congressional oversight committees.

(f) Initiation of programs

A special access program may not be initiated by a covered department or agency until—

- (1) the congressional oversight committees are notified of the program; and
- (2) a period of 30 days elapses after such notification is received.

(g) Definitions

For purposes of this section:

(1) Congressional oversight committees

The term “congressional oversight committees” means—

- (A) congressional leadership and authorizing and appropriations congressional committees with jurisdiction or shared jurisdiction over a department or agency;
- (B) the Committee on Homeland Security and Governmental Affairs of the Senate; and
- (C) the Committee on Oversight and Government Reform of the House of Representatives.

(2) Covered department or agency

(A) Except as provided in subparagraph (B), the term “covered department or agency” means any department or agency of the Federal Government that carries out a special access program.

(B) Such term does not include—

- (i) the Department of Defense (which is required to submit reports on special access programs under section 119 of title 10);
- (ii) the National Nuclear Security Administration (which is required to submit reports on special access programs under section 2426 of this title); or
- (iii) an agency in the Intelligence Community (as defined in section 3003(4) of this title).

(3) Special access program

The term “special access program” means any program that, under the authority of Executive Order 12356 (or any successor Executive order), is established by the head of a department or agency whom the President has designated in the Federal Register as an original “secret” or “top secret” classification authority that imposes “need-to-know” controls or access controls beyond those controls normally required (by regulations applicable to such department or agency) for access to information classified as “confidential”, “secret”, or “top secret”.

(Pub. L. 103-160, div. A, title XI, §1152, Nov. 30, 1993, 107 Stat. 1758; Pub. L. 106-65, div. C, title XXXII, §3294(e)(2), Oct. 5, 1999, 113 Stat. 970; Pub. L. 115-390, title I, §103, Dec. 21, 2018, 132 Stat. 5177.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 12356, referred to in subsec. (g)(3), is Ex. Ord. No. 12356, Apr. 2, 1982, 47 F.R. 14874, 15557, which prescribed a uniform system for classifying, declassifying, and safeguarding national security information, and which was formerly set out as a note under section 435 (now section 3161) of this title, was revoked by Ex. Ord. No. 12958, §6.1(d), Apr. 17, 1995, 60 F.R. 19843.

CODIFICATION

Section 103 of Pub. L. 115-390, which directed amendment of the National Defense Authorization Act for Fiscal Year 1994 (50 U.S.C. 3348), was executed to this section, which is section 1152 of the National Defense Authorization Act for Fiscal Year 1994 (Pub. L. 103-160), to reflect the probable intent of Congress. See 2018 Amendment notes below.

Section was formerly classified as a note under section 435 of this title prior to editorial reclassification as this section.

AMENDMENTS

2018—Subsecs. (a) to (e). Pub. L. 115–390, § 103(1), substituted “the congressional oversight committees” for “Congress” wherever appearing. See Codification note above.

Subsec. (f)(1). Pub. L. 115–390, § 103(2), substituted “congressional oversight committees” for “appropriate oversight committees”. See Codification note above.

Subsec. (g). Pub. L. 115–390, § 103(3), added par. (1) and redesignated former pars. (1) and (2) as (2) and (3), respectively. See Codification note above.

1999—Subsec. (g)(1)(B)(ii). Pub. L. 106–65 amended cl. (ii) generally. Prior to amendment, cl. (ii) read as follows: “the Department of Energy, with respect to special access programs carried out under the atomic energy defense activities of that department (for which the Secretary of Energy is required to submit reports under section 2122a of title 42); or”.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

EFFECTIVE DATE OF 1999 AMENDMENT

Amendment by Pub. L. 106–65 effective Mar. 1, 2000, see section 3299 of Pub. L. 106–65, set out as an Effective Date note under section 2401 of this title.

§ 3348a. Congressional oversight of sensitive programs not covered by other provisions of law

(a) Reports required

(1) In general

Not later than February 1 of each year, the head of each covered element shall submit to congressional leadership a report on each covered program carried out by that covered element.

(2) Contents

Each such report shall set forth—

(A) the total amount requested by the covered element for covered programs within the budget submitted under section 1105 of title 31 for the fiscal year following the fiscal year in which the report is submitted; and

(B) for each program in such budget that is a covered program—

- (i) a brief description of the program;
- (ii) in the case of a procurement program, a brief discussion of the major milestones established for the program;
- (iii) the actual cost of the program for each fiscal year during which the program has been conducted before the fiscal year during which that budget is submitted; and
- (iv) the estimated total cost of the program and the estimated cost of the program for—
 - (I) the current fiscal year;
 - (II) the fiscal year for which the budget is submitted; and
 - (III) each of the four succeeding fiscal years during which the program is expected to be conducted.

(b) Newly designated programs

(1) In general

Not later than February 1 of each year, the head of each covered element shall submit to congressional leadership a report that, with respect to each new covered program of that covered element, provides—

- (A) notice of the designation of the program as a special access program; and
- (B) justification for such designation.

(2) Contents

A report under paragraph (1) with respect to a program shall include—

- (A) the current estimate of the total program cost for the program; and
- (B) an identification, as applicable, of existing programs or technologies that are similar to the technology, or that have a mission similar to the technology, or that have a mission similar to the mission, of the program that is the subject of the notice.

(c) New covered program defined

In this subsection, the term “new covered program” means a covered program that has not previously been covered in a notice and justification under this subsection.

(c) Revision in classification of programs

(1) In general

Whenever a change in the classification of a covered program of a covered element is planned to be made or whenever classified information concerning a covered program of a covered element is to be declassified and made public, the head of the covered element shall submit to congressional leadership a report containing a description of the proposed change or the information to be declassified, the reasons for the proposed change or declassification, and notice of any public announcement planned to be made with respect to the proposed change or declassification.

(2) Period for submittal

Except as provided in paragraph (3), a report referred to in paragraph (1) shall be submitted not less than 14 days before the date on which the proposed change, declassification, or public announcement is to occur.

(3) Exception

If the head of the covered element determines that because of exceptional circumstances the requirement of paragraph (2) cannot be met with respect to a proposed change, declassification, or public announcement concerning a covered program of the covered element, the head of the department or agency may submit the report required by paragraph (1) regarding the proposed change, declassification, or public announcement at any time before the proposed change, declassification, or public announcement is made and shall include in the report an explanation of the exceptional circumstances.

(d) Revision of criteria for designating programs

Whenever there is a modification or termination of the policy and criteria used for designating a program of a covered element as a cov-

ered program, the head of the covered element shall promptly notify congressional leadership of such modification or termination. Any such notification shall contain the reasons for the modification or termination and, in the case of a modification, the provisions of the policy as modified.

(e) Initiation of programs

A covered program may not be initiated by a covered element until—

- (1) congressional leadership is notified of the program; and
- (2) a period of 30 days elapses after such notification is received.

(f) Limitation on use of funds

No funds may be obligated or expended by any covered element to carry out a covered program until the head of the covered element has briefed congressional leadership on the covered program.

(g) Definitions

In this section:

(1) Covered element

The term “covered element” means any element or portion of the Federal Government that is not—

- (A) a covered department or agency as defined in section 3348(g) of this title;
- (B) the Department of Defense (which is required to submit reports on special access programs under section 119 of title 10);
- (C) the National Nuclear Security Administration (which is required to submit reports on special access programs under section 2426 of this title); or
- (D) an element of the intelligence community (as defined in section 3003 of this title).

(2) Congressional leadership

The term “congressional leadership” means—

- (A) the majority leader of the Senate;
- (B) the minority leader of the Senate;
- (C) the Speaker of the House of Representatives; and
- (D) the minority leader of the House of Representatives.

(3) Covered program

The term “covered program” means any special access program or similarly protected program established under the authority of Executive Order 12356 (50 U.S.C. 3161 note; relating to prescribing a uniform system for classifying, declassifying, and safeguarding national security information), or any successor Executive order, or any similar sensitive program established anywhere in the Federal Government, including one established at the direction of the President.

(Pub. L. 117–103, div. HH, title V, §501, Mar. 15, 2022, 136 Stat. 1114.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 12356, referred to in subsec. (g)(3), is Ex. Ord. No. 12356, Apr. 2, 1982, 47 F.R. 14874, 15557, which was revoked by Ex. Ord. No. 12958, Apr. 17, 1995,

60 F.R. 19825, which was subsequently revoked by Ex. Ord. No. 13526, §6.2(g), Dec. 29, 2009, 75 F.R. 731. Ex. Ord. No. 13526, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information, is set out as a note under section 3161 of this title.

§ 3349. Notification regarding the authorized public disclosure of national intelligence

(a) Notification

In the event of an authorized disclosure of national intelligence or intelligence related to national security to the persons or entities described in subsection (b), the government official responsible for authorizing the disclosure shall submit to the congressional intelligence committees on a timely basis a notification of the disclosure if—

- (1) at the time of the disclosure—
 - (A) such intelligence is classified; or
 - (B) is declassified for the purpose of the disclosure; and

- (2) the disclosure will be made by an officer, employee, or contractor of the Executive branch.

(b) Persons or entities described

The persons or entities described in this subsection are as follows:

- (1) Media personnel.
- (2) Any person or entity, if the disclosure described in subsection (a) is made with the intent or knowledge that such information will be made publicly available.

(c) Content

Each notification required under subsection (a) shall—

- (1) provide the specific title and authority of the individual authorizing the disclosure;
- (2) if applicable, provide the specific title and authority of the individual who authorized the declassification of the intelligence disclosed; and
- (3) describe the intelligence disclosed, including the classification of the intelligence prior to its disclosure or declassification and the rationale for making the disclosure.

(d) Exception

The notification requirement in this section does not apply to a disclosure made—

- (1) pursuant to any statutory requirement, including to section 552 of title 5 (commonly referred to as the “Freedom of Information Act”);
- (2) in connection with a civil, criminal, or administrative proceeding;
- (3) as a result of a declassification review process under Executive Order 13526 (50 U.S.C. 435 note) [now 50 U.S.C. 3161 note] or any successor order; or
- (4) to any officer, employee, or contractor of the Federal government or member of an advisory committee to an element of the intelligence community who possesses an active security clearance and a need to know the specific national intelligence or intelligence related to national security, as defined in section 3003(5) of this title.

(Pub. L. 112–277, title V, §504, Jan. 14, 2013, 126 Stat. 2477; Pub. L. 113–126, title III, §328, July 7, 2014, 128 Stat. 1405.)

Editorial Notes**AMENDMENTS**

2014—Subsec. (e). Pub. L. 113–126 struck out subsec. (e). Text read as follows: “The notification requirements of this section shall cease to be effective for any disclosure described in subsection (a) that occurs on or after the date that is one year after January 14, 2013.”

Statutory Notes and Related Subsidiaries**DEFINITIONS**

Pub. L. 112–277, § 2, Jan. 14, 2013, 126 Stat. 2469, provided that: “In this Act [see Tables for classification]:

“(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ‘congressional intelligence committees’ means—

“(A) the Select Committee on Intelligence of the Senate; and

“(B) the Permanent Select Committee on Intelligence of the House of Representatives.

“(2) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)) [now 50 U.S.C. 3003(4)].”

§ 3350. Maximum amount charged for declassification reviews

In reviewing and processing a request by a person for the mandatory declassification of information pursuant to Executive Order No. 13526, a successor executive order, or any provision of law, the head of an element of the intelligence community—

(1) may not charge the person reproduction fees in excess of the amount of fees that the head would charge the person for reproduction required in the course of processing a request for information under section 552 of title 5 (commonly referred to as the “Freedom of Information Act”); and

(2) may waive or reduce any processing fees in the same manner as the head waives or reduces fees under such section 552.

(Pub. L. 115–31, div. N, title III, § 313, May 5, 2017, 131 Stat. 816.)

Editorial Notes**REFERENCES IN TEXT**

Executive Order No. 13526, referred to in text, is Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, 1013, which is set out as a note under section 3161 of this title.

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definition of “intelligence community” as used in this section, see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3350a. Promoting efficient declassification review**(a) In general**

Whenever an agency is processing a request pursuant to section 552 of title 5 (commonly known as the “Freedom of Information Act”) or the mandatory declassification review provisions of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or successor order, and identifies responsive classified records that are more than 25

years of age as of December 31 of the year in which the request is received, the head of the agency shall, in accordance with existing processes to protect national security under the Freedom of Information Act and the mandatory review provisions of Executive Order 12526,¹ review the record and process the record for declassification and release by the National Declassification Center of the National Archives and Records Administration, unless the head of agency—

(1) makes a certification to Congress, including the congressional intelligence committees, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on the Judiciary of the Senate, and the Committee on Armed Services, the Committee on Oversight and Accountability, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives, that the declassification of certain components within the record would be harmful to the protection of sources and methods or national security, pursuant to existing processes; and

(2) provides an explanation to Congress, including the congressional intelligence committees, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on the Judiciary of the Senate, and the Committee on Armed Services, the Committee on Oversight and Accountability, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives, for such certification.

(b) Application

Subsection (a) shall apply regardless of whether or not the record described in such subsection is in the legal custody of the National Archives and Records Administration.

(Pub. L. 118–31, div. G, title VI, § 7602, Dec. 22, 2023, 137 Stat. 1096.)

Editorial Notes**REFERENCES IN TEXT**

Executive Order 13526, referred to in subsec. (a), is Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, 1013, which is set out as a note under section 3161 of this title.

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definition of “congressional intelligence committees” as used in this section, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.

§ 3351. Improving quality of information in background investigation request packages**(a) Report on metrics and best practices**

Not later than 180 days after December 20, 2019, the Director of the Defense Counterintelligence and Security Agency, which serves as the primary executive branch service provider for background investigations for eligibility for

¹ So in original. Probably should be “13526.”

access to classified information, eligibility to hold a sensitive position, and for suitability and fitness for other matters pursuant to Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for Government employment, fitness for contractor employees, and eligibility for access to classified national security information), shall, in consultation with the Security, Suitability, and Credentialing Performance Accountability Council established under such executive order, submit to Congress a report on—

(1) metrics for assessing the completeness and quality of packages for background investigations submitted by agencies requesting background investigations from the Defense Counterintelligence and Security Agency;

(2) rejection rates of background investigation submission packages due to incomplete or erroneous data, by agency; and

(3) best practices for ensuring full and complete information in background investigation requests.

(b) Annual report on performance

Not later than 270 days after December 20, 2019, and not less frequently than once each year thereafter, the Security, Suitability, and Credentialing Performance Accountability Council shall submit to Congress a report on performance against the metrics and return rates identified in paragraphs (1) and (2) of subsection (a).

(c) Improvement plans

(1) Identification

Not later than one year after December 20, 2019, executive agents under Executive Order 13467 (50 U.S.C. 3161 note) shall identify agencies in need of improvement with respect to the quality of the information in the background investigation submissions of the agencies as reported in subsection (b).

(2) Plans

Not later than 90 days after an agency is identified under paragraph (1), the head of the agency shall provide the executive agents referred to in such paragraph with a plan to improve the performance of the agency with respect to the quality of the information in the agency's background investigation submissions.

(Pub. L. 116–92, div. A, title XVII, §1757, Dec. 20, 2019, 133 Stat. 1860.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13467, referred to in subsecs. (a) and (c)(1), is Ex. Ord. No. 13467, June 30, 2008, 73 F.R. 38103, which is set out as a note under section 3161 of this title.

§ 3351a. Making certain policies and execution plans relating to personnel clearances available to industry partners

(a) Definitions

In this section:

(1) Security executive agent

The term “Security Executive Agent” means the officer serving as the Security Ex-

ecutive Agent pursuant to section 3162a of this title.

(2) Appropriate industry partner

The term “appropriate industry partner” means a contractor, licensee, or grantee (as defined in section 101(a) of Executive Order 12829 (50 U.S.C. 3161 note; relating to National Industrial Security Program), as in effect on the day before December 20, 2019) that is participating in the National Industrial Security Program established by such Executive Order.

(b) Sharing of policies and plans required

Each head of a Federal agency shall share policies and plans relating to security clearances with appropriate industry partners directly affected by such policies and plans in a manner consistent with the protection of national security as well as the goals and objectives of the National Industrial Security Program administered pursuant to Executive Order 12829 (50 U.S.C. 3161 note; relating to the National Industrial Security Program).

(c) Development of policies and procedures required

Not later than 90 days after December 20, 2019, the Security Executive Agent and the Director of the National Industrial Security Program shall jointly develop policies and procedures by which appropriate industry partners with proper security clearances and a need to know can have appropriate access to the policies and plans shared pursuant to subsection (b) that directly affect those industry partners.

(Pub. L. 116–92, div. E, title LIV, §5402, Dec. 20, 2019, 133 Stat. 2143.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 12829, referred to in subsecs. (a)(2) and (b), is Ex. Ord. No. 12829, Jan. 6, 1993, 58 F.R. 3479, which is set out as a note under section 3161 of this title.

§ 3351b. Limitations on determinations regarding certain security classifications

(a) Prohibition

An officer of an element of the intelligence community who has been nominated by the President for a position that requires the advice and consent of the Senate may not make a classification decision with respect to information related to such officer's nomination.

(b) Classification determinations

(1) In general

Except as provided in paragraph (2), in a case in which an officer described in subsection (a) has been nominated as described in such subsection and classification authority rests with the officer or another officer who reports directly to such officer, a classification decision with respect to information relating to the officer shall be made by the Director of National Intelligence.

(2) Nominations of Director of National Intelligence

In a case described in paragraph (1) in which the officer nominated is the Director of Na-

tional Intelligence, the classification decision shall be made by the Principal Deputy Director of National Intelligence.

(c) Reports

Whenever the Director or the Principal Deputy Director makes a decision under subsection (b), the Director or the Principal Deputy Director, as the case may be, shall submit to the congressional intelligence committees a report detailing the reasons for the decision.

(Pub. L. 116-92, div. E, title LXIII, § 6310, Dec. 20, 2019, 133 Stat. 2190.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3352. Definitions

In this title:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

- (A) the congressional intelligence committees;
- (B) the Committee on Armed Services of the Senate;
- (C) the Committee on Appropriations of the Senate;
- (D) the Committee on Homeland Security and Governmental Affairs of the Senate;
- (E) the Committee on Armed Services of the House of Representatives;
- (F) the Committee on Appropriations of the House of Representatives;
- (G) the Committee on Homeland Security of the House of Representatives; and
- (H) the Committee on Oversight and Reform of the House of Representatives.

(2) Appropriate industry partner

The term “appropriate industry partner” means a contractor, licensee, or grantee (as defined in section 101(a) of Executive Order No. 12829 (50 U.S.C. 3161 note; relating to National Industrial Security Program)) that is participating in the National Industrial Security Program established by such Executive order.

(3) Continuous vetting

The term “continuous vetting” has the meaning given such term in Executive Order No. 13467 (50 U.S.C. 3161 note; relating to reforming processes for determining suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information).

(4) Council

The term “Council” means the Security, Suitability, and Credentialing Performance Accountability Council established pursuant to such Executive order, or any successor entity.

(5) Reciprocity

The term “reciprocity” means reciprocal recognition by Federal departments and agen-

cies of eligibility for access to classified information.

(6) Security Executive Agent

The term “Security Executive Agent” means the officer serving as the Security Executive Agent pursuant to section 3162a of this title.

(7) Suitability and Credentialing Executive Agent

The term “Suitability and Credentialing Executive Agent” means the Director of the Office of Personnel Management acting as the Suitability and Credentialing Executive Agent in accordance with Executive Order No. 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for Government employment, fitness for contractor employees, and eligibility for access to classified national security information), or any successor entity.

(Pub. L. 116-92, div. E, title LXVI, § 6601, Dec. 20, 2019, 133 Stat. 2209.)

Editorial Notes

REFERENCES IN TEXT

This title, referred to in text, means title LXVI of div. E of Pub. L. 116-92, which enacted this section and sections 3162a and 3352a to 3352f of this title and amended sections 3033, 3104, 3163, and 3164 of this title. For complete classification of title LXVI to the Code, see Tables.

Executive Order No. 12829, referred to in par. (2), is Ex. Ord. No. 12829, Jan. 6, 1993, 58 F.R. 3479, which is set out as a note under section 3161 of this title.

Executive Order No. 13467, referred to in pars. (3), (4), and (7), is Ex. Ord. No. 13467, June 30, 2008, 73 F.R. 38103, which is set out as a note under section 3161 of this title.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3352a. Reports and plans relating to security clearances and background investigations

(a) Sense of Congress

It is the sense of Congress that—

- (1) ensuring the trustworthiness and security of the workforce, facilities, and information of the Federal Government is of the highest priority to national security and public safety;
- (2) the President and Congress should prioritize the modernization of the personnel security framework to improve its efficiency, effectiveness, and accountability;
- (3) the current system for background investigations for security clearances, suitability and fitness for employment, and credentialing

lacks efficiencies and capabilities to meet the current threat environment, recruit and retain a trusted workforce, and capitalize on modern technologies; and

(4) changes to policies or processes to improve this system should be vetted through the Council to ensure standardization, portability, and reciprocity in security clearances across the Federal Government.

(b) Accountability plans and reports

(1) Plans

Not later than 90 days after December 20, 2019, the Council shall submit to the appropriate congressional committees and make available to appropriate industry partners the following:

(A) A plan, with milestones, to reduce the background investigation inventory to 200,000, or an otherwise sustainable steady-level, by the end of year 2020. Such plan shall include notes of any required changes in investigative and adjudicative standards or resources.

(B) A plan to consolidate the conduct of background investigations associated with the processing for security clearances in the most effective and efficient manner in the Defense Counterintelligence and Security Agency. Such plan shall address required funding, personnel, contracts, information technology, field office structure, policy, governance, schedule, transition costs, and effects on stakeholders.

(2) Report on the future of personnel security

(A) In general

Not later than 180 days after December 20, 2019, the Chairman of the Council, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a report on the future of personnel security to reflect changes in threats, the workforce, and technology.

(B) Contents

The report submitted under subparagraph (A) shall include the following:

(i) A risk framework for granting and renewing access to classified information.

(ii) A discussion of the use of technologies to prevent, detect, and monitor threats.

(iii) A discussion of efforts to address reciprocity and portability.

(iv) A discussion of the characteristics of effective insider threat programs.

(v) An analysis of how to integrate data from continuous vetting, insider threat programs, and human resources data.

(vi) Recommendations on interagency governance.

(3) Plan for implementation

Not later than 180 days after December 20, 2019, the Chairman of the Council, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a plan to implement the re-

port's framework and recommendations submitted under paragraph (2)(A).

(4) Congressional notifications

Not less frequently than quarterly, the Security Executive Agent shall make available to the public a report regarding the status of the disposition of requests received from departments and agencies of the Federal Government for a change to, or approval under, the Federal investigative standards, the national adjudicative guidelines, continuous vetting, or other national policy regarding personnel security.

(Pub. L. 116–92, div. E, title LXVI, § 6602, Dec. 20, 2019, 133 Stat. 2210.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “Council”, “reciprocity”, “appropriate congressional committees”, “appropriate industry partners”, “continuous vetting”, and “Security Executive Agent”, referred to in text, see section 3352 of this title.

§ 3352b. Improving the process for security clearances

(a) Reviews

Not later than 180 days after December 20, 2019, the Security Executive Agent, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a report that includes the following:

(1) A review of whether the information requested on the Questionnaire for National Security Positions (Standard Form 86) and by the Federal Investigative Standards prescribed by the Suitability and Credentialing Executive Agent and the Security Executive Agent appropriately supports the adjudicative guidelines under Security Executive Agent Directive 4 (known as the “National Security Adjudicative Guidelines”). Such review shall include identification of whether any such information currently collected is unnecessary to support the adjudicative guidelines.

(2) An assessment of whether such Questionnaire, Standards, and guidelines should be revised to account for the prospect of a holder of a security clearance becoming an insider threat.

(3) Recommendations to improve the background investigation process by—

(A) simplifying the Questionnaire for National Security Positions (Standard Form 86) and increasing customer support to applicants completing such Questionnaire;

(B) using remote techniques and centralized locations to support or replace field investigation work;

(C) using secure and reliable digitization of information obtained during the clearance process;

(D) building the capacity of the background investigation workforce; and

(E) replacing periodic reinvestigations with continuous vetting techniques in all appropriate circumstances.

(b) Policy, strategy, and implementation

Not later than 180 days after December 20, 2019, the Security Executive Agent shall, in coordination with the members of the Council, establish the following:

(1) A policy and implementation plan for the issuance of interim security clearances.

(2) A policy and implementation plan to ensure contractors are treated consistently in the security clearance process across agencies and departments of the United States as compared to employees of such agencies and departments. Such policy shall address—

(A) prioritization of processing security clearances based on the mission the contractors will be performing;

(B) standardization in the forms that agencies issue to initiate the process for a security clearance;

(C) digitization of background investigation-related forms;

(D) use of the polygraph;

(E) the application of the adjudicative guidelines under Security Executive Agent Directive 4 (known as the “National Security Adjudicative Guidelines”);

(F) reciprocal recognition of clearances across agencies and departments of the United States, regardless of status of periodic reinvestigation;

(G) tracking of clearance files as individuals move from employment with an agency or department of the United States to employment in the private sector;

(H) collection of timelines for movement of contractors across agencies and departments;

(I) reporting on security incidents and job performance, consistent with section 552a of title 5 (commonly known as the “Privacy Act of 1974”), that may affect the ability to hold a security clearance;

(J) any recommended changes to the Federal Acquisition Regulations (FAR) necessary to ensure that information affecting contractor clearances or suitability is appropriately and expeditiously shared between and among agencies and contractors; and

(K) portability of contractor security clearances between or among contracts at the same agency and between or among contracts at different agencies that require the same level of clearance.

(3) A strategy and implementation plan that—

(A) provides for periodic reinvestigations as part of a security clearance determination only on an as-needed, risk-based basis;

(B) includes actions to assess the extent to which automated records checks and other continuous vetting methods may be used to expedite or focus reinvestigations; and

(C) provides an exception to the requirement under subparagraph (A) for certain populations if the Security Executive Agent—

(i) determines such populations require reinvestigations at regular intervals; and

(ii) provides written justification to the appropriate congressional committees for any such determination.

(4) A policy and implementation plan for agencies and departments of the United States, as a part of the security clearance process, to accept automated records checks generated pursuant to a security clearance applicant’s employment with a prior employer.

(5) A policy for the use of certain background information on individuals collected by the private sector for background investigation purposes.

(6) Uniform standards for agency continuous vetting programs to ensure quality and reciprocity in accepting enrollment in a continuous vetting program as a substitute for a periodic investigation for continued access to classified information.

(Pub. L. 116–92, div. E, title LXVI, § 6603, Dec. 20, 2019, 133 Stat. 2211.)

Statutory Notes and Related Subsidiaries**IMPROVING VISIBILITY INTO THE SECURITY CLEARANCE PROCESS**

Pub. L. 116–92, div. E, title LIV, § 5401, Dec. 20, 2019, 133 Stat. 2142, provided that:

“(a) **DEFINITION OF SECURITY EXECUTIVE AGENT.**—In this section, the term ‘Security Executive Agent’ means the officer serving as the Security Executive Agent pursuant to section 803 of the National Security Act of 1947 [50 U.S.C. 3162a], as added by section 6605.

“(b) **POLICY REQUIRED.**—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Security Executive Agent shall issue a policy that requires the head of each Federal agency to create, not later than December 31, 2023, an electronic portal that can be used by human resources personnel and applicants for security clearances to view information about the status of an application for a security clearance and the average time required for each phase of the security clearance process.”

DEFINITIONS

For definitions of “Security Executive Agent”, “Council”, “appropriate congressional committees”, “appropriate industry partners”, “Suitability and Credentialing Executive Agent”, “continuous vetting”, and “reciprocity”, referred to in text, see section 3352 of this title.

§ 3352c. Goals for promptness of determinations regarding security clearances**(a) In general**

The Council shall reform the security clearance process with the objective that, by December 31, 2021, 90 percent of all determinations, other than determinations regarding populations identified under section 3352b(b)(3)(C) of this title, regarding—

(1) security clearances—

(A) at the secret level are issued in 30 days or fewer; and

(B) at the top secret level are issued in 90 days or fewer; and

(2) reciprocity of security clearances at the same level are recognized in 2 weeks or fewer.

(b) Certain reinvestigations

The Council shall reform the security clearance process with the goal that by December 31, 2021, reinvestigation on a set periodicity is not required for more than 10 percent of the population that holds a security clearance.

(c) Equivalent metrics**(1) In general**

If the Council develops a set of performance metrics that it certifies to the appropriate congressional committees should achieve substantially equivalent outcomes as those outlined in subsections (a) and (b), the Council may use those metrics for purposes of compliance within this provision.

(2) Notice

If the Council uses the authority provided by paragraph (1) to use metrics as described in such paragraph, the Council shall, not later than 30 days after communicating such metrics to departments and agencies, notify the appropriate congressional committees that it is using such authority.

(d) Plan

Not later than 180 days after December 20, 2019, the Council shall submit to the appropriate congressional committees and make available to appropriate industry partners a plan to carry out this section. Such plan shall include recommended interim milestones for the goals set forth in subsections (a) and (b) for 2019, 2020, and 2021.

(Pub. L. 116–92, div. E, title LXVI, § 6604, Dec. 20, 2019, 133 Stat. 2213; Pub. L. 117–263, div. F, title LXVIII, § 6824(b)(3), Dec. 23, 2022, 136 Stat. 3615.)

Editorial Notes**AMENDMENTS**

2022—Subsecs. (c)(1), (d). Pub. L. 117–263 substituted “subsections (a) and (b)” for “subsections (b) and (c)”.

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definitions of “Council”, “reciprocity”, “appropriate congressional committees”, and “appropriate industry partners”, referred to in text, see section 3352 of this title.

§ 3352d. Reports on reciprocity for security clearances inside of departments and agencies**(a) Reports to Security Executive Agent**

The head of each Federal department or agency shall submit an annual report to the Security Executive Agent that, with respect to the period covered by the report—

(1) identifies the number of individuals whose security clearances took more than 2 weeks for reciprocity recognition after such individuals move to another part of such department or agency; and

(2) breaks out the information described in paragraph (1) by type of clearance and the reasons for any delays.

(b) Annual report

Not less frequently than once each year, the Security Executive Agent shall submit to the appropriate congressional committees and make available to industry partners a report that summarizes the information received pursuant to subsection (b) during the period covered by such report.

(Pub. L. 116–92, div. E, title LXVI, § 6608, Dec. 20, 2019, 133 Stat. 2216.)

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definitions of “Security Executive Agent”, “reciprocity”, and “appropriate congressional committees”, referred to in text, see section 3352 of this title.

§ 3352e. Periodic report on positions in the intelligence community that can be conducted without access to classified information, networks, or facilities

Not later than 180 days after December 20, 2019, and biennially thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a report that reviews the intelligence community for which positions can be conducted without access to classified information, networks, or facilities, or may only require a security clearance at the secret level. Such report shall take into account the potential effect of maintaining continuity of operations during a covered national emergency (as defined by section 3316b of this title) and the assessed needs of the intelligence community to maintain such continuity of operations.

(Pub. L. 116–92, div. E, title LXVI, § 6610, Dec. 20, 2019, 133 Stat. 2218; Pub. L. 117–103, div. X, title VIII, § 801, Mar. 15, 2022, 136 Stat. 1011.)

Editorial Notes**AMENDMENTS**

2022—Pub. L. 117–103 substituted “December 20, 2019, and biennially thereafter,” for “December 20, 2019, and not less frequently than once every 5 years thereafter,” and inserted at end “Such report shall take into account the potential effect of maintaining continuity of operations during a covered national emergency (as defined by section 3316b of this title) and the assessed needs of the intelligence community to maintain such continuity of operations.”

Statutory Notes and Related Subsidiaries**DEFINITIONS**

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

§ 3352f. Information-sharing program for positions of trust and security clearances**(a) Program required****(1) In general**

Not later than 90 days after December 20, 2019, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall establish and implement a program to share between and among agencies of the Federal Government and industry partners of the Federal Government relevant background information regarding individuals applying for and currently occupying national security positions and positions of trust, in order to ensure the Federal Government maintains a trusted workforce.

(2) Designation

The program established under paragraph (1) shall be known as the “Trusted Information Provider Program” (in this section referred to as the “Program”).

(b) Privacy safeguards

The Security Executive Agent and the Suitability and Credentialing Executive Agent shall ensure that the Program includes such safeguards for privacy as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate.

(c) Provision of information to the Federal Government

The Program shall include requirements that enable investigative service providers and agencies of the Federal Government to leverage certain pre-employment information gathered through private-sector means during the employment or military recruiting process, and other relevant security or human resources information obtained during employment with or for the Federal Government, that satisfy Federal investigative standards, while safeguarding personnel privacy.

(d) Information and records

The information and records considered under the Program shall include the following:

- (1) Date and place of birth.
- (2) Citizenship or immigration and naturalization information.
- (3) Education records.
- (4) Employment records.
- (5) Employment or social references.
- (6) Military service records.
- (7) State and local law enforcement checks.
- (8) Criminal history checks.
- (9) Financial records or information.
- (10) Foreign travel, relatives, or associations.
- (11) Social media checks.
- (12) Such other information or records as may be relevant to obtaining or maintaining national security, suitability, fitness, or credentialing eligibility.

(e) Implementation plan**(1) In general**

Not later than 90 days after December 20, 2019, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a plan for the implementation of the Program.

(2) Elements

The plan required by paragraph (1) shall include the following:

(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate to carry out or improve the Program.

(f) Plan for pilot program on two-way information sharing**(1) In general**

Not later than 180 days after December 20, 2019, the Security Executive Agent and the

Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a plan for the implementation of a pilot program to assess the feasibility and advisability of expanding the Program to include the sharing of information held by the Federal Government related to contract personnel with the security office of the employers of those contractor personnel.

(2) Elements

The plan required by paragraph (1) shall include the following:

(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate to carry out or improve the pilot program.

(g) Review

Not later than 1 year after December 20, 2019, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a review of the plans submitted under subsections (e)(1) and (f)(1) and utility and effectiveness of the programs described in such plans.

(Pub. L. 116–92, div. E, title LXVI, § 6611, Dec. 20, 2019, 133 Stat. 2218.)

Statutory Notes and Related Subsidiaries**FEDERAL POLICY ON SHARING OF COVERED INSIDER THREAT INFORMATION PERTAINING TO CONTRACTOR EMPLOYEES IN THE TRUSTED WORKFORCE**

Pub. L. 117–103, div. X, title VIII, § 806, Mar. 15, 2022, 136 Stat. 1014, as amended by Pub. L. 117–263, div. F, title LXVI, § 6606, Dec. 23, 2022, 136 Stat. 3559, provided that:

“(a) **POLICY REQUIRED.**—Not later than 2 years after the date of the enactment of this Act [Mar. 15, 2022], the Director of National Intelligence, in coordination with the Secretary of Defense, the Director of the Office of Management and Budget, and the Attorney General, shall issue a policy for the Federal Government on sharing covered insider threat information pertaining to contractor employees.

“(b) **CONSENT REQUIREMENT.**—The Director shall ensure that the policy issued under subsection (a) requires, as a condition of obtaining and maintaining a security clearance with the Federal Government, that a contractor employee provide prior written consent for the Federal Government to share covered insider threat information with the senior official responsible for the insider threat program of the contractor that employs the contractor employee. The Director may include in such policy restrictions on the further disclosure of such information.

“(c) **CONSULTATION.**—On a quarterly basis during the period in which the Director is developing the policy under subsection (a), the Director shall consult with Congress and industry partners with respect to such development.

“(d) **REVIEW.**—

“(1) **SUBMISSION.**—Not later than 1 year after the date of the issuance of the policy under subsection

(a), the Director of National Intelligence and the Secretary of Defense shall jointly submit to Congress and make available to such industry partners as the Director and the Secretary consider appropriate a review of the policy.

“(2) CONTENTS.—The review under paragraph (1) shall include the following:

“(A) An assessment of the utility and effectiveness of the policy issued under subsection (a).

“(B) Such recommendations as the Director and the Secretary determine appropriate with respect to legislative or administrative action relevant to such policy.

“(e) DEFINITIONS.—In this section:

“(1) COVERED INSIDER THREAT INFORMATION.—The term ‘covered insider threat information’—

“(A) means information that—

“(i) is relevant with respect to adjudications relating to determinations of eligibility for access to classified information;

“(ii) an agency or department of the Federal Government has vetted and verified; and

“(iii) according to Director of National Intelligence policy, is considered relevant to the ability of a contractor employee to protect against insider threats as required by section 117.7(d) of title 32, Code of Federal Regulations, or successor regulation; and

“(B) includes pertinent information considered in the counter-threat assessment, as authorized by a provision of Federal law or Executive Order.

“(2) CONTRACTOR EMPLOYEE.—The term ‘contractor employee’ means an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a department or agency of the Federal Government.”

GOVERNANCE OF TRUSTED WORKFORCE 2.0 INITIATIVE

Pub. L. 117–103, div. X, title VIII, §807(a), Mar. 15, 2022, 136 Stat. 1015, provided that:

“(a) GOVERNANCE.—The Director of National Intelligence, acting as the Security Executive Agent, and the Director of the Office of Personnel Management, acting as the Suitability and Credentialing Executive Agent, in coordination with the Deputy Director for Management in the Office of Management and Budget, acting as the chairman of the Performance Accountability Council, and the Under Secretary of Defense for Intelligence and Security shall jointly—

“(1) not later than 180 days after the date of the enactment of this Act [Mar. 15, 2022], publish, in the Federal Register as appropriate, a policy with guidelines and standards for Federal Government agencies and industry partners to implement the Trusted Workforce 2.0 initiative;

“(2) not later than 2 years after the date of the enactment of this Act and not less frequently than once every 6 months thereafter, submit to Congress a report on the timing, delivery, and adoption of Federal Government agencies’ policies, products, and services to implement the Trusted Workforce 2.0 initiative, including those associated with the National Background Investigation Service; and

“(3) not later than 90 days after the date of the enactment of this Act, submit to Congress performance management metrics for the implementation of the Trusted Workforce 2.0 initiative, including performance metrics regarding timeliness, cost, and measures of effectiveness.”

TRUSTED INFORMATION PROVIDER PROGRAM FOR NATIONAL SECURITY POSITIONS AND POSITIONS OF TRUST

Pub. L. 115–232, div. A, title IX, §941, Aug. 13, 2018, 132 Stat. 1941, provided that:

“(a) PROGRAM REQUIRED.—Not later than 90 days after the date of the enactment of this Act [Aug. 13, 2018], the Security Executive Agent and the Suitability/Credentialing Executive Agent shall establish and implement a program (to be known as the ‘Trusted Infor-

mation Provider Program’) to share between and among agencies of the Federal Government and industry partners of the Federal Government relevant background information regarding individuals applying for and currently occupying national security positions and positions of trust, in order to ensure the Federal Government maintains a trusted workforce.

“(b) PRIVACY SAFEGUARDS.—The Security Executive Agent and the Suitability/Credentialing Executive Agent shall ensure that the program required by subsection (a) includes such safeguards for privacy as the Security Executive Agent and the Suitability/Credentialing Executive Agent consider appropriate.

“(c) PROVISION OF INFORMATION TO THE FEDERAL GOVERNMENT.—The program required by subsection (a) shall include requirements that enable Investigative Service Providers and agencies of the Federal Government to leverage certain pre-employment information gathered during the employment or military recruiting process, and other relevant security or human resources information obtained during employment with or for the Federal Government, that satisfy Federal investigative standards, while safeguarding personnel privacy.

“(d) INFORMATION AND RECORDS.—The information and records considered under the program required by subsection (a) shall include the following:

“(1) Date and place of birth.

“(2) Citizenship or immigration and naturalization information.

“(3) Education records.

“(4) Employment records.

“(5) Employment or social references.

“(6) Military service records.

“(7) State and local law enforcement checks.

“(8) Criminal history checks.

“(9) Financial records or information.

“(10) Foreign travel, relatives or associations.

“(11) Social media checks.

“(12) Any other information or records relevant to obtaining or maintaining national security, suitability, fitness, or credentialing eligibility.

“(e) IMPLEMENTATION PLAN.—

“(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Aug. 13, 2018], the Security Executive Agent and the Suitability/Credentialing Executive Agent shall jointly submit to Congress a plan for the implementation of the program required by subsection (a).

“(2) ELEMENTS.—The plan required by paragraph (1) shall include the following:

“(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

“(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability/Credentialing Executive Agent consider appropriate to carry out or improve the program.

“(f) DEFINITIONS.—In this section:

“(1) The term ‘Security Executive Agent’ means the Director of National Intelligence acting as the Security Executive Agent in accordance with Executive Order 13467 (73 Fed. Reg. 38103; 50 U.S.C. 3161 note).

“(2) The term ‘Suitability/Credentialing Executive Agent’ means the Director of the Office of Personnel Management acting as the Suitability/Credentialing Executive Agent in accordance with Executive Order 13467.”

DEFINITIONS

For definitions of “Security Executive Agent”, “Suitability and Credentialing Executive Agent”, “appropriate congressional committees”, and “appropriate industry partners”, referred to in text, see section 3352 of this title.

§ 3352g. Requirement to authorize additional security clearances for certain contractors

(a) Definitions

In this section:

(1) Appropriate committees of Congress

The term “appropriate committees of Congress” means—

- (A) the congressional intelligence committees;
- (B) the Subcommittee on Defense of the Committee on Appropriations of the Senate; and
- (C) the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

(2) Covered contract or agreement

The term “covered contract or agreement”, with respect to an entity, means a contract or other agreement between that entity and an element of the intelligence community the performance of which requires a specified number of covered persons to hold a security clearance.

(3) Covered person

The term “covered person”, with respect to an entity, means a contractor or employee of that entity.

(b) Plan and study**(1) In general**

No later than April 1, 2024, the Director of National Intelligence shall—

- (A) complete a study on the feasibility and advisability of implementing a program to authorize additional security clearances for certain contractors as described in subsection (c);
- (B) develop a plan to implement the program described in subparagraph (A); and
- (C) submit to the appropriate committees of Congress—
 - (i) a report on the findings of the Director with respect to the study completed pursuant to subparagraph (A); and
 - (ii) the plan developed pursuant to subparagraph (B).

(2) Study elements

The study completed pursuant to paragraph (1)(A) shall address the following:

- (A) For contracts agreed to after December 22, 2023, how private entities that contract with the intelligence community would make payments for additional clearances for their employees and how the intelligence community would receive payments.
- (B) A list of and changes to provisions of law required in order to fully implement the program required by subsection (c) and achieve the intent indicated in subparagraph (A) of this paragraph.
- (C) Such considerations as the Director may have for carrying out the program required by subsection (c) and achieving the intent indicated in subparagraph (A) of this paragraph.

(c) Program to authorize additional security clearances for certain contractors

Subject to the limitations described in subsection (d), the Director shall establish a program under which—

- (1) any entity that enters into a covered contract or agreement with an element of the in-

telligence community may designate an additional number of covered persons who may submit an application for a security clearance;

(2) the appropriate authorized investigative agency and authorized adjudicative agency, as such terms are defined in section 3341(a) of this title, shall—

(A) upon receiving such an application—

- (i) conduct an appropriate investigation of the background of the additional covered person; and
- (ii) make a determination as to whether the additional covered person is eligible for access to classified information; and

(B) if the determination under subparagraph (A)(ii) is favorable, upon any of the specified number of covered persons required to hold a security clearance for the performance of work under that covered contract or agreement becoming unable to perform such work, make a determination as to whether the additional covered person has a demonstrated need-to-know under Executive Order 12968 (60 Fed. Reg. 40245; relating to access to classified information), or any successor thereto, or Executive Order 10865 (25 Fed. Reg. 1583; relating to safeguarding classified information within industry), or any successor thereto (without requiring an additional investigation to be conducted under subparagraph (A)(i)); and

(3) if the additional covered person receives a favorable determination regarding the need-to-know under paragraph (2)(B) and signs an approved nondisclosure agreement, the additional covered person may perform such work in lieu of such covered person.

(d) Limitations

The limitations described in this subsection are as follows:

(1) Limitation on number designated per contract

The additional number designated by an entity under the program established pursuant to subsection (c) for each covered contract or agreement may not exceed the greater of the following:

- (A) 10 percent of the number of security clearances required to be held by covered persons to perform work under the covered contract or agreement.
- (B) 1 person.

(2) Limitation on number designated per entity

The total additional number designated by an entity under the program established pursuant to subsection (c) may not exceed the greater of the following:

- (A) 10 percent of the sum total number of security clearances required to be held by covered persons to perform work under all covered contracts or agreements of the entity.
- (B) 1 person.

(e) Prohibitions**(1) In general**

No application for a security clearance may be submitted by a covered person of an entity

or granted pursuant to the program established under subsection (c) in excess of the limitations under subsection (d) applicable to such entity.

(2) Prohibition on bearing costs

No head of an element of the intelligence community may bear any cost associated with granting or maintaining a security clearance the application for which is submitted pursuant to subsection (c)(1).

(f) Rule of construction

Nothing in this section may be construed as requiring the head of an element of the intelligence community to grant any covered person access to classified information if a favorable determination of eligibility to access such classified information is not made with respect to such person.

(Pub. L. 118–31, div. G, title V, § 7505, Dec. 22, 2023, 137 Stat. 1084.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 12968, referred to in subsec. (c)(2)(B), is Ex. Ord. No. 12968, Aug. 2, 1995, 60 F.R. 40245, which is set out as a note under section 3161 of this title.

Executive Order 10865, referred to in subsec. (c)(2)(B), is Ex. Ord. No. 10865, Feb. 20, 1960, 25 F.R. 1583, which is set out as a note under section 3161 of this title.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.

§ 3352h. Timeliness standard for rendering determinations of trust for personnel vetting

(a) Timeliness standard

(1) In general

The President shall, acting through the Security Executive Agent and the Suitability and Credentialing Executive Agent, establish and publish in such public venue as the President considers appropriate, new timeliness performance standards for processing personnel vetting trust determinations in accordance with the Federal personnel vetting performance management standards.

(2) Quinquennial reviews

Not less frequently than once every 5 years, the President shall, acting through the Security Executive Agent and the Suitability and Credentialing Executive Agent—

(A) review the standards established pursuant to paragraph (1); and

(B) pursuant to such review—

(i) update such standards as the President considers appropriate; and

(ii) publish in the Federal Register such updates as may be made pursuant to clause (i).

(3) Omitted

(b) Quarterly reports on implementation

(1) In general

Not less frequently than quarterly, the Security Executive Agent and the Suitability and

Credentialing Executive Agent shall jointly make available to the public a quarterly report on the compliance of Executive agencies (as defined in section 105 of title 5) with the standards established pursuant to subsection (a).

(2) Disaggregation

Each report made available pursuant to paragraph (1) shall disaggregate, to the greatest extent practicable, data by appropriate category of personnel risk and between Government and contractor personnel.

(c) Complementary standards for intelligence community

The Director of National Intelligence may, in consultation with the Security, Suitability, and Credentialing Performance Accountability Council established pursuant to Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for Government employment, fitness for contractor employees, and eligibility for access to classified national security information) establish for the intelligence community standards complementary to those established pursuant to subsection (a).

(d) Data with respect to timeliness of polygraph examinations

(1) In general

With respect to each report on compliance with timeliness standards for rendering determinations of trust for personnel vetting prepared pursuant to subsection (b), the Director of National Intelligence shall make available to the congressional intelligence committees as soon as practicable anonymized raw data with respect to the timeliness of polygraph examinations used to prepare each such report in machine-readable format for each element of the intelligence community that collects such data.

(2) Form and classification justification

The data provided to the congressional intelligence committees under paragraph (1) may be modified to remove any personally identifying information, shall be submitted in unclassified form to the greatest extent possible, and shall contain a justification for the classification of any such data provided.

(Pub. L. 118–31, div. G, title VII, § 7702, Dec. 22, 2023, 137 Stat. 1100; Pub. L. 118–159, div. F, title LXVI, § 6604, Dec. 23, 2024, 138 Stat. 2503.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13467, referred to in subsec. (c), is Ex. Ord. No. 13467, June 30, 2008, 73 F.R. 38103, which is set out as a note under section 3161 of this title.

CODIFICATION

Section is comprised of section 7702 of Pub. L. 118–31. Subsec. (a)(3) of section 7702 of Pub. L. 118–31 amended section 3341 of this title.

AMENDMENTS

2024—Subsec. (d). Pub. L. 118–159 added subsec. (d).

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 7002 of Pub. L. 118-31, set out as a note under section 3003 of this title.

SUBCHAPTER III—A—PUBLIC INTEREST DECLASSIFICATIONS**§ 3355. Findings**

Congress makes the following findings:

(1) It is in the national interest to establish an effective, coordinated, and cost-effective means by which records on specific subjects of extraordinary public interest that do not undermine the national security interests of the United States may be collected, retained, reviewed, and disseminated to Congress, policy-makers in the executive branch, and the public.

(2) Ensuring, through such measures, public access to information that does not require continued protection to maintain the national security interests of the United States is a key to striking the balance between secrecy essential to national security and the openness that is central to the proper functioning of the political institutions of the United States.

(Pub. L. 106-567, title VII, § 702, Dec. 27, 2000, 114 Stat. 2856.)

Editorial Notes**CODIFICATION**

Section was formerly set out in a note under section 3161 of this title.

Statutory Notes and Related Subsidiaries**EFFECTIVE DATE**

Pub. L. 106-567, title VII, § 710, Dec. 27, 2000, 114 Stat. 2864, as amended by Pub. L. 108-458, title I, § 1102(f), Dec. 17, 2004, 118 Stat. 3700; Pub. L. 110-53, title VI, § 602(4), Aug. 3, 2007, 121 Stat. 336; Pub. L. 112-235, § 2(c), Dec. 28, 2012, 126 Stat. 1626; Pub. L. 113-126, title III, § 311, July 7, 2014, 128 Stat. 1399; Pub. L. 116-92, div. E, title LXVII, § 6741(b), Dec. 20, 2019, 133 Stat. 2239, provided that: “This title [enacting this subchapter] shall take effect on the date that is 120 days after the date of the enactment of this Act [Dec. 27, 2000].”

SHORT TITLE

For short title of title VII of Pub. L. 106-567, which enacted this subchapter, as the “Public Interest Declassification Act of 2000”, see section 701 of Pub. L. 106-567, set out as a note under section 3301 of this title.

STATUS OF BOARD

Pub. L. 116-92, div. E, title LXVII, § 6741(c), Dec. 20, 2019, 133 Stat. 2239, provided that: “Notwithstanding section 710(b) of the Public Interest Declassification Act of 2000 (Public Law 106-567; 50 U.S.C. 3161 note) as in effect on the day before the date of the enactment of this Act [Dec. 20, 2019]—

“(1) the Public Interest Declassification Board shall be deemed to not have terminated for purposes of the appointment of members to the Board;

“(2) section 703(h) of such Act [50 U.S.C. 3355a(h)] shall not apply with respect to the period beginning on December 31, 2018, and ending on the day before the date of the enactment of this Act; and

“(3) the length of the terms of the members serving on the Board as of December 30, 2018, shall be cal-

culated by not counting the period specified in paragraph (2).”

[Prior to being struck out by Pub. L. 116-92, div. E, title LXVII, § 6741(b)(1), Dec. 20, 2019, 133 Stat. 2239, section 710(b) of the Public Interest Declassification Act of 2000 (Pub. L. 106-567, title VII), referred to in the introductory provisions of section 6741(c) of Pub. L. 116-92, set out above, provided that: “The provisions of this title shall expire on December 31, 2018.” Section 710 of the Act was formerly set out in a note under section 3161 of this title, and was editorially transferred and is now set out as an Effective Date note above.]

§ 3355a. Public Interest Declassification Board**(a) Establishment**

(1) There is established within the executive branch of the United States a board to be known as the “Public Interest Declassification Board” (in this subchapter referred to as the “Board”).

(2) The Board shall report directly to the President or, upon designation by the President, the Vice President, the Attorney General, or other designee of the President. The other designee of the President under this paragraph may not be an agency head or official authorized to classify information under Executive Order 13526, or any successor order.

(b) Purposes

The purposes of the Board are as follows:

(1) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release to Congress, interested agencies, and the public of declassified records and materials (including donated historical materials) that are of archival value, including records and materials of extraordinary public interest.

(2) To promote the fullest possible public access to a thorough, accurate, and reliable documentary record of significant United States national security decisions and significant United States national security activities in order to—

(A) support the oversight and legislative functions of Congress;

(B) support the policymaking role of the executive branch;

(C) respond to the interest of the public in national security matters; and

(D) promote reliable historical analysis and new avenues of historical study in national security matters.

(3) To provide recommendations to the President for the identification, collection, and review for declassification of information of extraordinary public interest that does not undermine the national security of the United States, to be undertaken in accordance with a declassification program that has been established or may be established by the President by Executive order.

(4) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on

policies deriving from the issuance by the President of Executive orders regarding the classification and declassification of national security information.

(5) To review and make recommendations to the President in a timely manner with respect to any congressional request, made by the committee of jurisdiction or by a member of the committee of jurisdiction, to declassify certain records, to evaluate the proper classification of certain records, or to reconsider a declination to declassify specific records.

(c) Membership

(1) The Board shall be composed of nine individuals appointed from among citizens of the United States who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or archives, including individuals who have served in Congress or otherwise in the Federal Government or have otherwise engaged in research, scholarship, or publication in such fields on matters relating to the national security of the United States, of whom—

(A) five shall be appointed by the President;

(B) one shall be appointed by the Speaker of the House of Representatives;

(C) one shall be appointed by the majority leader of the Senate;

(D) one shall be appointed by the minority leader of the Senate; and

(E) one shall be appointed by the minority leader of the House of Representatives.

(2)(A) Of the members initially appointed to the Board by the President—

(i) three shall be appointed for a term of 4 years;

(ii) one shall be appointed for a term of 3 years; and

(iii) one shall be appointed for a term of 2 years.

(B) The members initially appointed to the Board by the Speaker of the House of Representatives or by the majority leader of the Senate shall be appointed for a term of 3 years.

(C) The members initially appointed to the Board by the minority leader of the House of Representatives or the Senate shall be appointed for a term of 2 years.

(D) Any subsequent appointment to the Board shall be for a term of 3 years from the date of the appointment.

(3) A vacancy in the Board shall be filled in the same manner as the original appointment.

(4) A member of the Board may be appointed to a new term on the Board upon the expiration of the member's term on the Board, except that no member may serve more than three full terms on the Board.

(5) A member of the Board whose term has expired may continue to serve until the earlier of—

(A) the date that a successor is appointed and sworn in; and

(B) the date that is 1 year after the date of the expiration of the term.

(6) Not later than 30 days after the date on which the term of a member of the Board ends, the appointing authority of the member shall

submit to Congress a plan to appoint a successor.

(d) Chairperson; Executive Secretary

(1)(A) The President shall designate one of the members of the Board as the Chairperson of the Board.

(B) The term of service as Chairperson of the Board shall be 2 years.

(C) A member serving as Chairperson of the Board may be redesignated as Chairperson of the Board upon the expiration of the member's term as Chairperson of the Board, except that no member shall serve as Chairperson of the Board for more than 6 years.

(2) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Board.

(e) Meetings

The Board shall meet as needed to accomplish its mission, consistent with the availability of funds, but shall meet in person not less frequently than on a quarterly basis. A majority of the members of the Board shall constitute a quorum.

(f) Staff

(1) Any employee of the Federal Government may be detailed to the Board, with the agreement of and without reimbursement to the detailing agency, and such detail shall be without interruption or loss of civil, military, or foreign service status or privilege.

(2) In addition to any employees detailed to the Board under paragraph (1), the Board may, subject to the availability of funds, hire not more than 12 staff members.

(g) Security

(1) The members and staff of the Board shall, as a condition of appointment to or employment with the Board, hold appropriate security clearances for access to the classified records and materials to be reviewed by the Board or its staff, and shall follow the guidance and practices on security under applicable Executive orders and Presidential or agency directives.

(2) The head of an agency shall, as a condition of granting access to a member of the Board, the Executive Secretary of the Board, or a member of the staff of the Board to classified records or materials of the agency under this subchapter, require the member, the Executive Secretary, or the member of the staff, as the case may be, to—

(A) execute an agreement regarding the security of such records or materials that is approved by the head of the agency; and

(B) hold an appropriate security clearance granted or recognized under the standard procedures and eligibility criteria of the agency, including any special access approval required for access to such records or materials.

(3) The members of the Board, the Executive Secretary of the Board, and the members of the staff of the Board may not use any information acquired in the course of their official activities on the Board for nonofficial purposes.

(4) For purposes of any law or regulation governing access to classified information that pertains to the national security of the United States, and subject to any limitations on access

arising under section 3355d(b) of this title, and to facilitate the advisory functions of the Board under this subchapter, a member of the Board seeking access to a record or material under this subchapter shall be deemed for purposes of this subsection to have a need to know the contents of the record or material.

(h) Compensation

(1) Each member of the Board shall receive compensation at a rate not to exceed the daily equivalent of the annual rate of basic pay payable for positions at ES-1 of the Senior Executive Service under section 5382 of title 5 for each day such member is engaged in the actual performance of duties of the Board.

(2) Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, while away from their homes or regular places of business in the performance of the duties of the Board.

(i) Guidance; annual budget

(1) On behalf of the President, the Assistant to the President for National Security Affairs shall provide guidance on policy to the Board.

(2) The Executive Secretary of the Board, under the direction of the Chairperson of the Board and the Board, and acting in consultation with the Archivist of the United States, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget, shall prepare the annual budget of the Board.

(j) Support

The Information Security Oversight Office may support the activities of the Board under this subchapter. Such support shall be provided on a reimbursable basis.

(k) Public availability of records and reports

(1) The Board shall make available for public inspection records of its proceedings and reports prepared in the course of its activities under this subchapter to the extent such records and reports are not classified and would not be exempt from release under the provisions of section 552 of title 5.

(2) In making records and reports available under paragraph (1), the Board shall coordinate the release of such records and reports with appropriate officials from agencies with expertise in classified information in order to ensure that such records and reports do not inadvertently contain classified information.

(l) Applicability of certain administrative laws

The provisions of chapter 10 of title 5 shall not apply to the activities of the Board under this subchapter. However, the records of the Board shall be governed by the provisions of the Federal Records Act of 1950.

(Pub. L. 106-567, title VII, § 703, Dec. 27, 2000, 114 Stat. 2856; Pub. L. 108-458, title I, § 1102(a), (b), Dec. 17, 2004, 118 Stat. 3699; Pub. L. 111-259, title III, § 365, Oct. 7, 2010, 124 Stat. 2702; Pub. L. 112-235, § 2(a), (b), Dec. 28, 2012, 126 Stat. 1626; Pub. L. 116-92, div. E, title LXVII, § 6741(a), Dec. 20, 2019, 133 Stat. 2239; Pub. L. 117-263, div. F,

title LXVIII, § 6824(d)(1), Dec. 23, 2022, 136 Stat. 3615; Pub. L. 117-286, § 4(a)(318), Dec. 27, 2022, 136 Stat. 4341; Pub. L. 118-31, div. G, title VI, § 7604, Dec. 22, 2023, 137 Stat. 1097.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13526, referred to in subsec. (a)(2), is set out as a note under section 3161 of this title.

The Federal Records Act of 1950, referred to in subsec. (l), was title V of act June 30, 1949, ch. 288, as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583, which was classified generally to sections 392 to 396 and 397 to 401 of former Title 44, Public Printing and Documents. Section 6(d) of act Sept. 5, 1950, was repealed by Pub. L. 90-620, Oct. 22, 1968, 82 Stat. 1238, the first section of which enacted Title 44, Public Printing and Documents. For disposition of sections of former Title 44, see Table at the beginning of Title 44. Title V of act June 30, 1949, was repealed by Pub. L. 107-217, § 4, Aug. 21, 2002, 116 Stat. 1303.

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

AMENDMENTS

2023—Subsec. (c)(5), (6). Pub. L. 118-31, § 7604(1), added pars. (5) and (6).

Subsec. (f). Pub. L. 118-31, § 7604(2), designated existing provisions as par. (1) and added par. (2).

2022—Subsec. (a)(2). Pub. L. 117-263 substituted “Executive Order 13526” for “Executive Order 12958”.

Subsec. (l). Pub. L. 117-286 substituted “chapter 10 of title 5” for “the Federal Advisory Committee Act (5 U.S.C. App.)”.

2019—Subsec. (e). Pub. L. 116-92 substituted “funds, but shall meet in person not less frequently than on a quarterly basis.” for “funds.”

2012—Subsec. (c)(2)(D). Pub. L. 112-235, § 2(a), substituted “from the date of the appointment.” for period at end.

Subsec. (c)(3). Pub. L. 112-235, § 2(b), struck out at end “A member of the Board appointed to fill a vacancy before the expiration of a term shall serve for the remainder of the term.”

2010—Subsec. (b)(5). Pub. L. 111-259 substituted “jurisdiction or by a member of the committee of jurisdiction,” for “jurisdiction,” and inserted “, to evaluate the proper classification of certain records,” after “certain records”.

2004—Subsec. (a). Pub. L. 108-458, § 1102(a), designated existing provisions as par. (1) and added par. (2).

Subsec. (b)(5). Pub. L. 108-458, § 1102(b), added par. (5).

§ 3355b. Identification, collection, and review for declassification of information of archival value or extraordinary public interest

(a) Briefings on agency declassification programs

(1) As requested by the Board, or by the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives, the head of any agency with the authority under an Executive order to classify information shall provide to the Board, the Select Committee on Intelligence of the Senate, or the Permanent Select Committee on Intelligence of the House of Representatives, on an annual basis, a summary briefing and report on such agency's progress and plans in the declassification of national security information. Such briefing shall cover the declassification goals set by statute, regula-

tion, or policy, the agency's progress with respect to such goals, and the agency's planned goals and priorities for its declassification activities over the next 2 fiscal years. Agency briefings and reports shall give particular attention to progress on the declassification of records and materials that are of archival value or extraordinary public interest to the people of the United States.

(2)(A) The annual briefing and report under paragraph (1) for agencies within the Department of Defense, including the military departments and the elements of the intelligence community, shall be provided on a consolidated basis.

(B) In this paragraph, the term "elements of the intelligence community" means the elements of the intelligence community specified or designated under section 3003(4) of this title.

(b) Recommendations on agency declassification programs

(1) Upon reviewing and discussing declassification plans and progress with an agency, the Board shall provide to the head of the agency the written recommendations of the Board as to how the agency's declassification program could be improved. A copy of each recommendation shall also be submitted to the Assistant to the President for National Security Affairs and the Director of the Office of Management and Budget.

(2) Consistent with the provisions of section 3355a(k) of this title, the Board's recommendations to the head of an agency under paragraph (1) shall become public 60 days after such recommendations are sent to the head of the agency under that paragraph.

(c) Recommendations on special searches for records of extraordinary public interest

(1) The Board shall also make recommendations to the President regarding proposed initiatives to identify, collect, and review for declassification classified records and materials of extraordinary public interest.

(2) In making recommendations under paragraph (1), the Board shall consider the following:

(A) The opinions and requests of Members of Congress, including opinions and requests expressed or embodied in letters or legislative proposals, and also including specific requests for the declassification of certain records or for the reconsideration of declinations to declassify specific records.

(B) The opinions and requests of the National Security Council, the Director of National Intelligence, and the heads of other agencies.

(C) The opinions of United States citizens.

(D) The opinions of members of the Board.

(E) The impact of special searches on systematic and all other on-going declassification programs.

(F) The costs (including budgetary costs) and the impact that complying with the recommendations would have on agency budgets, programs, and operations.

(G) The benefits of the recommendations.

(H) The impact of compliance with the recommendations on the national security of the United States.

(d) President's declassification priorities

(1) Concurrent with the submission to Congress of the budget of the President each fiscal year under section 1105 of title 31, the Director of the Office of Management and Budget shall publish a description of the President's declassification program and priorities, together with a listing of the funds requested to implement that program.

(2) Nothing in this subchapter shall be construed to substitute or supersede, or establish a funding process for, any declassification program that has been established or may be established by the President by Executive order.

(e) Declassification reviews

(1) In general

If requested by the President, the Board shall review in a timely manner certain records or declinations to declassify specific records, the declassification of which has been the subject of specific congressional request described in section 3355a(b)(5) of this title.

(2) Authority of board

Upon receiving a congressional request described in section 3355a(b)(5) of this title, the Board may conduct the review and make the recommendations described in that section, regardless of whether such a review is requested by the President.

(3) Reporting

Any recommendations submitted to the President by the Board under section 3355a(b)(5) of this title shall be submitted to the chairman and ranking minority member of the committee of Congress that made the request relating to such recommendations.

(Pub. L. 106-567, title VII, § 704, Dec. 27, 2000, 114 Stat. 2859; Pub. L. 108-458, title I, § 1102(c), (d), Dec. 17, 2004, 118 Stat. 3699; Pub. L. 110-53, title VI, § 602(1), (2), Aug. 3, 2007, 121 Stat. 335; Pub. L. 117-263, div. F, title LXVIII, § 6824(d)(2), Dec. 23, 2022, 136 Stat. 3615.)

Editorial Notes

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

AMENDMENTS

2022—Subsec. (e)(3). Pub. L. 117-263 struck out comma before "shall".

2007—Subsec. (c)(2)(B). Pub. L. 110-53, § 602(1), substituted "Director of National Intelligence" for "Director of Central Intelligence".

Subsec. (e). Pub. L. 110-53, § 602(2), designated existing provisions as par. (1), inserted par. (1) heading, and added pars. (2) and (3).

2004—Subsec. (c)(2)(A). Pub. L. 108-458, § 1102(c), inserted before period at end "and also including specific requests for the declassification of certain records or for the reconsideration of declinations to declassify specific records".

Subsec. (e). Pub. L. 108-458, § 1102(d), added subsec. (e).

§ 3355c. Protection of national security information and other information

(a) In general

Nothing in this subchapter shall be construed to limit the authority of the head of an agency

to classify information or to continue the classification of information previously classified by that agency.

(b) Special access programs

Nothing in this subchapter shall be construed to limit the authority of the head of an agency to grant or deny access to a special access program.

(c) Authorities of Director of National Intelligence

Nothing in this subchapter shall be construed to limit the authorities of the Director of National Intelligence as the head of the intelligence community, including the Director's responsibility to protect intelligence sources and methods from unauthorized disclosure as required by section 3024(i) of this title.

(d) Exemptions to release of information

Nothing in this subchapter shall be construed to limit any exemption or exception to the release to the public under this subchapter of information that is protected under subsection (b) of section 552 of title 5 (commonly referred to as the "Freedom of Information Act"), or section 552a of title 5 (commonly referred to as the "Privacy Act").

(e) Withholding information from Congress

Nothing in this subchapter shall be construed to authorize the withholding of information from Congress.

(Pub. L. 106-567, title VII, § 705, Dec. 27, 2000, 114 Stat. 2861; Pub. L. 110-53, title VI, § 602(1), (3), Aug. 3, 2007, 121 Stat. 335, 336; Pub. L. 117-263, div. F, title LXVIII, § 6824(d)(3), Dec. 23, 2022, 136 Stat. 3615.)

Editorial Notes

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

AMENDMENTS

2022—Subsec. (c). Pub. L. 117-263 substituted "section 3024(i) of this title" for "section 103(c)(6) of the National Security Act of 1947".

2007—Subsec. (c). Pub. L. 110-53 substituted "Director of National Intelligence" for "Director of Central Intelligence" in heading and text.

§ 3355d. Standards and procedures

(a) Liaison

(1) The head of each agency with the authority under an Executive order to classify information and the head of each Federal Presidential library shall designate an employee of such agency or library to act as liaison to the Board for purposes of this subchapter.

(2) The Board may establish liaison and otherwise consult with such other historical and advisory committees as the Board considers appropriate for purposes of this subchapter.

(b) Limitations on access

(1)(A) Except as provided in paragraph (2), if the head of an agency or the head of a Federal Presidential library determines it necessary to deny or restrict access of the Board, or of the

agency or library liaison to the Board, to information contained in a record or material, in whole or in part, the head of the agency or the head of the library shall promptly notify the Board in writing of such determination.

(B) Each notice to the Board under subparagraph (A) shall include a description of the nature of the records or materials, and a justification for the determination, covered by such notice.

(2) In the case of a determination referred to in paragraph (1) with respect to a special access program created by the Secretary of Defense, the Director of National Intelligence, or the head of any other agency, the notification of denial of access under paragraph (1), including a description of the nature of the Board's request for access, shall be submitted to the Assistant to the President for National Security Affairs rather than to the Board.

(c) Discretion to disclose

At the conclusion of a declassification review, the head of an agency may, in the discretion of the head of the agency, determine that the public's interest in the disclosure of records or materials of the agency covered by such review, and still properly classified, outweighs the Government's need to protect such records or materials, and may release such records or materials in accordance with the provisions of Executive Order 13526 or any successor order to such Executive order.

(d) Discretion to protect

At the conclusion of a declassification review, the head of an agency may, in the discretion of the head of the agency, determine that the interest of the agency in the protection of records or materials of the agency covered by such review, and still properly classified, outweighs the public's need for access to such records or materials, and may deny release of such records or materials in accordance with the provisions of Executive Order 13526 or any successor order to such Executive order.

(e) Reports

(1)(A) Except as provided in paragraph (2), the Board shall annually submit to the appropriate congressional committees a report on the activities of the Board under this subchapter, including summary information regarding any denials to the Board by the head of an agency or the head of a Federal Presidential library of access to records or materials under this subchapter.

(B) In this paragraph, the term "appropriate congressional committees" means the Select Committee on Intelligence and the Committee on Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Government Reform of the House of Representatives.

(2) Notwithstanding paragraph (1), notice that the Board has been denied access to records and materials, and a justification for the determination in support of the denial, shall be submitted by the agency denying the access as follows:

(A) In the case of the denial of access to a special access program created by the Secretary of Defense, to the Committees on Armed Services and Appropriations of the

Senate and to the Committees on Armed Services and Appropriations of the House of Representatives.

(B) In the case of the denial of access to a special access program created by the Director of National Intelligence, or by the head of any other agency (including the Department of Defense) if the special access program pertains to intelligence activities, or of access to any information and materials relating to intelligence sources and methods, to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(C) In the case of the denial of access to a special access program created by the Secretary of Energy or the Administrator for Nuclear Security, to the Committees on Armed Services and Appropriations and the Select Committee on Intelligence of the Senate and to the Committees on Armed Services and Appropriations and the Permanent Select Committee on Intelligence of the House of Representatives.

(f) Notification of review

In response to a specific congressional request for declassification review described in section 3355a(b)(5) of this title, the Board shall advise the originators of the request in a timely manner whether the Board intends to conduct such review.

(Pub. L. 106–567, title VII, § 706, Dec. 27, 2000, 114 Stat. 2861; Pub. L. 108–458, title I, § 1102(e), Dec. 17, 2004, 118 Stat. 3700; Pub. L. 110–53, title VI, § 602(1), Aug. 3, 2007, 121 Stat. 335; Pub. L. 117–263, div. F, title LXVIII, § 6824(d)(4), Dec. 23, 2022, 136 Stat. 3615.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13526, referred to in subsecs. (c) and (d), is set out as a note under section 3161 of this title.

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

AMENDMENTS

2022—Subsecs. (c), (d). Pub. L. 117–263 substituted “Executive Order 13526” for “Executive Order No. 12958”.

2007—Subsecs. (b)(2), (e)(2)(B). Pub. L. 110–53 substituted “Director of National Intelligence” for “Director of Central Intelligence”.

2004—Subsec. (f). Pub. L. 108–458 added subsec. (f).

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Government Reform of the House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

Committee on Governmental Affairs of the Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

§ 3355e. Judicial review

Nothing in this subchapter limits the protection afforded to any information under any other provision of law. This subchapter is not intended and may not be construed to create any right or benefit, substantive or procedural, enforceable against the United States, its agencies, its officers, or its employees. This subchapter does not modify in any way the substantive criteria or procedures for the classification of information, nor does this subchapter create any right or benefit subject to judicial review.

(Pub. L. 106–567, title VII, § 707, Dec. 27, 2000, 114 Stat. 2862.)

Editorial Notes

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

§ 3355f. Funding

(a) Authorization of appropriations

There is hereby authorized to be appropriated to carry out the provisions of this subchapter amounts as follows:

(1) For fiscal year 2001, \$650,000.

(2) For each fiscal year after fiscal year 2001, such sums as may be necessary for such fiscal year.

(b) Funding requests

The President shall include in the budget submitted to Congress for each fiscal year under section 1105 of title 31 a request for amounts for the activities of the Board under this subchapter during such fiscal year.

(Pub. L. 106–567, title VII, § 708, Dec. 27, 2000, 114 Stat. 2863.)

Editorial Notes

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

§ 3355g. Definitions

In this subchapter:

(1) Agency

(A) Except as provided in subparagraph (B), the term “agency” means the following:

(i) An Executive agency, as that term is defined in section 105 of title 5.

(ii) A military department, as that term is defined in section 102 of such title.

(iii) Any other entity in the executive branch that comes into the possession of classified information.

(B) The term does not include the Board.

(2) Classified material or record

The terms “classified material” and “classified record” include any correspondence,

memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine readable records, and other documentary material, regardless of physical form or characteristics, that has been determined pursuant to Executive order to require protection against unauthorized disclosure in the interests of the national security of the United States.

(3) Declassification

The term “declassification” means the process by which records or materials that have been classified are determined no longer to require protection from unauthorized disclosure to protect the national security of the United States.

(4) Donated historical material

The term “donated historical material” means collections of personal papers donated or given to a Federal Presidential library or other archival repository under a deed of gift or otherwise.

(5) Federal Presidential library

The term “Federal Presidential library” means a library operated and maintained by the United States Government through the National Archives and Records Administration under the applicable provisions of the Federal Records Act of 1950.

(6) National security

The term “national security” means the national defense or foreign relations of the United States.

(7) Records or materials of extraordinary public interest

The term “records or materials of extraordinary public interest” means records or materials that—

(A) demonstrate and record the national security policies, actions, and decisions of the United States, including—

(i) policies, events, actions, and decisions which led to significant national security outcomes; and

(ii) the development and evolution of significant United States national security policies, actions, and decisions;

(B) will provide a significantly different perspective in general from records and materials publicly available in other historical sources; and

(C) would need to be addressed through ad hoc record searches outside any systematic declassification program established under Executive order.

(8) Records of archival value

The term “records of archival value” means records that have been determined by the Archivist of the United States to have sufficient historical or other value to warrant their continued preservation by the Federal Government.

(Pub. L. 106-567, title VII, § 709, Dec. 27, 2000, 114 Stat. 2863.)

Editorial Notes

REFERENCES IN TEXT

The Federal Records Act of 1950, referred to in par. (5), was title V of act June 30, 1949, ch. 288, as added Sept. 5, 1950, ch. 849, § 6(d), 64 Stat. 583, which was classified generally to sections 392 to 396 and 397 to 401 of former Title 44, Public Printing and Documents. Section 6(d) of act Sept. 5, 1950, was repealed by Pub. L. 90-620, Oct. 22, 1968, 82 Stat. 1238, the first section of which enacted Title 44, Public Printing and Documents. For disposition of sections of former Title 44, see Table at the beginning of Title 44. Title V of act June 30, 1949, was repealed by Pub. L. 107-217, § 4, Aug. 21, 2002, 116 Stat. 1303.

CODIFICATION

Section was formerly set out in a note under section 3161 of this title.

SUBCHAPTER IV—COLLECTION, ANALYSIS, AND SHARING OF INTELLIGENCE

§ 3361. National Virtual Translation Center

(a) Establishment

The Director of National Intelligence shall establish in the intelligence community an element with the function of connecting the elements of the intelligence community engaged in the acquisition, storage, translation, or analysis of voice or data in digital form.

(b) Designation

The element established under subsection (a) shall be known as the National Virtual Translation Center.

(c) Function

The element established under subsection (a) shall provide for timely and accurate translations of foreign intelligence for all elements of the intelligence community through—

(1) the integration of the translation capabilities of the intelligence community;

(2) the use of remote-connection capabilities; and

(3) the use of such other capabilities as the Director considers appropriate.

(d) Administrative matters

(1) The Director shall retain direct supervision and control over the element established under subsection (a).

(2) The element established under subsection (a) shall connect elements of the intelligence community utilizing the most current available information technology that is applicable to the function of the element.

(3) Personnel of the element established under subsection (a) may carry out the duties and functions of the element at any location that—

(A) has been certified as a secure facility by a department or agency of the United States Government; or

(B) the Director has otherwise determined to be appropriate for such duties and functions.

(e) Deadline for establishment

The element required by subsection (a) shall be established as soon as practicable after November 27, 2002, but not later than 90 days after November 27, 2002.

(Pub. L. 107-306, title III, § 313, Nov. 27, 2002, 116 Stat. 2391; Pub. L. 108-458, title I,

§ 1071(g)(2)(A)(i), Dec. 17, 2004, 118 Stat. 3691; Pub. L. 108-487, title III, § 304, Dec. 23, 2004, 118 Stat. 3944; Pub. L. 118-31, div. G, title IX, § 7901(f)(1), Dec. 22, 2023, 137 Stat. 1107.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 404n of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2023—Subsec. (d)(3)(B). Pub. L. 118-31 inserted period at end.

2004—Subsec. (a). Pub. L. 108-458 substituted “Director of National Intelligence” for “Director of Central Intelligence, acting as the head of the intelligence community.”.

Subsec. (c). Pub. L. 108-487, § 304(a)(2), added subsec. (c). Former subsec. (c) redesignated (d).

Subsec. (d). Pub. L. 108-487, § 304(a)(1), (b), redesignated subsec. (c) as (d) and added par. (3). Former subsec. (d) redesignated (e).

Subsec. (e). Pub. L. 108-487, § 304(a)(1), redesignated subsec. (d) as (e).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108-458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108-458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

§ 3362. Foreign Terrorist Asset Tracking Center

(a) Establishment

The Director of National Intelligence shall establish within the Central Intelligence Agency an element responsible for conducting all-source intelligence analysis of information relating to the financial capabilities, practices, and activities of individuals, groups, and nations associated with international terrorism in their activities relating to international terrorism.

(b) Designation

The element established under subsection (a) shall be known as the Foreign Terrorist Asset Tracking Center.

(c) Deadline for establishment

The element required by subsection (a) shall be established as soon as practicable after November 27, 2002, but not later than 90 days after November 27, 2002.

(Pub. L. 107-306, title III, § 341, Nov. 27, 2002, 116 Stat. 2398; Pub. L. 108-458, title I, § 1071(g)(2)(C), Dec. 17, 2004, 118 Stat. 3691.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 404n-1 of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2004—Subsec. (a). Pub. L. 108-458 substituted “Director of National Intelligence shall establish within the

Central Intelligence Agency” for “Director of Central Intelligence, acting as the head of the intelligence community, shall establish in the Central Intelligence Agency”.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108-458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108-458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

§ 3363. Terrorist Identification Classification System

(a) Requirement

(1) The Director of National Intelligence shall—

(A) establish and maintain a list of individuals who are known or suspected international terrorists, and of organizations that are known or suspected international terrorist organizations; and

(B) ensure that pertinent information on the list is shared with the departments, agencies, and organizations described by subsection (c).

(2) The list under paragraph (1), and the mechanisms for sharing information on the list, shall be known as the “Terrorist Identification Classification System”.

(b) Administration

(1) The Director shall prescribe requirements for the inclusion of an individual or organization on the list required by subsection (a), and for the deletion or omission from the list of an individual or organization currently on the list.

(2) The Director shall ensure that the information utilized to determine the inclusion, or deletion or omission, of an individual or organization on or from the list is derived from all-source intelligence.

(3) The Director shall ensure that the list is maintained in accordance with existing law and regulations governing the collection, storage, and dissemination of intelligence concerning United States persons.

(c) Information sharing

Subject to section 3024(i) of this title, relating to the protection of intelligence sources and methods, the Director shall provide for the sharing of the list, and information on the list, with such departments and agencies of the Federal Government, State and local government agencies, and entities of foreign governments and international organizations as the Director considers appropriate.

(d) Report on criteria for information sharing

(1) Not later than March 1, 2003, the Director shall submit to the congressional intelligence committees a report describing the criteria used to determine which types of information on the list required by subsection (a) are to be shared, and which types of information are not to be

shared, with various departments and agencies of the Federal Government, State and local government agencies, and entities of foreign governments and international organizations.

(2) The report shall include a description of the circumstances in which the Director has determined that sharing information on the list with the departments and agencies of the Federal Government, and of State and local governments, described by subsection (c) would be inappropriate due to the concerns addressed by section 403-3(c)(7)¹ of this title, relating to the protection of sources and methods, and any instance in which the sharing of information on the list has been inappropriate in light of such concerns.

(e) System administration requirements

(1) The Director shall, to the maximum extent practicable, ensure the interoperability of the Terrorist Identification Classification System with relevant information systems of the departments and agencies of the Federal Government, and of State and local governments, described by subsection (c).

(2) The Director shall ensure that the System utilizes technologies that are effective in aiding the identification of individuals in the field.

(f) Report on status of System

(1) Not later than one year after November 27, 2002, the Director shall, in consultation with the Director of Homeland Security, submit to the congressional intelligence committees a report on the status of the Terrorist Identification Classification System. The report shall contain a certification on the following:

(A) Whether the System contains the intelligence information necessary to facilitate the contribution of the System to the domestic security of the United States.

(B) Whether the departments and agencies having access to the System have access in a manner that permits such departments and agencies to carry out appropriately their domestic security responsibilities.

(C) Whether the System is operating in a manner that maximizes its contribution to the domestic security of the United States.

(D) If a certification under subparagraph (A), (B), or (C) is in the negative, the modifications or enhancements of the System necessary to ensure a future certification in the positive.

(2) The report shall be submitted in unclassified form, but may include a classified annex.

(g) Congressional intelligence committees defined

In this section, the term “congressional intelligence committees” means—

(1) the Select Committee on Intelligence of the Senate; and

(2) the Permanent Select Committee on Intelligence of the House of Representatives.

(Pub. L. 107-306, title III, §343, Nov. 27, 2002, 116 Stat. 2399; Pub. L. 108-177, title III, §377(d), Dec. 13, 2003, 117 Stat. 2631; Pub. L. 108-458, title I, §§1071(g)(2)(A)(ii), 1072(d)(1)(A), Dec. 17, 2004, 118 Stat. 3691, 3693; Pub. L. 111-259, title III, §347(f),

Oct. 7, 2010, 124 Stat. 2699; Pub. L. 118-31, div. G, title IX, §7901(f)(2), Dec. 22, 2023, 137 Stat. 1107.)

Editorial Notes

REFERENCES IN TEXT

Section 403-3 of this title, referred to in subsec. (d)(2), was repealed and a new section 403-3 enacted by Pub. L. 108-458, title I, §1011(a), Dec. 17, 2004, 118 Stat. 3643, without corresponding amendment to this section. Section 403-3 of this title was subsequently editorially reclassified as section 3025 of this title. The new section 3025 contains a subsec. (c) relating to the composition of the Office of the Director of National Intelligence.

CODIFICATION

Section was formerly classified to section 404n-2 of this title prior to editorial reclassification and renumbering as this section. Some section numbers of this title referenced in amendment notes below reflect the classification of such sections prior to their editorial reclassification.

AMENDMENTS

2023—Subsec. (d)(1). Pub. L. 118-31 substituted “Not later than” for “Not later then”.

2010—Subsecs. (d) to (h). Pub. L. 111-259 redesignated subsecs. (e) to (h) as (d) to (g), respectively, and struck out former subsec. (d). Prior to amendment, text of subsec. (d) read as follows:

“(1) The Director shall review on an annual basis the information provided by various departments and agencies for purposes of the list under subsection (a) in order to determine whether or not the information so provided is derived from the widest possible range of intelligence available to such departments and agencies.

“(2) The Director shall, as a result of each review under paragraph (1), certify whether or not the elements of the intelligence community responsible for the collection of intelligence related to the list have provided information for purposes of the list that is derived from the widest possible range of intelligence available to such department and agencies.”

2004—Subsec. (a)(1). Pub. L. 108-458, §1071(g)(2)(A)(ii), which directed amendment of par. (1) by substituting “Director of National Intelligence” for “Director of Central Intelligence, acting as the head of the intelligence community,” was executed by making the substitution for “Director of Central Intelligence, acting as head of the Intelligence Community,” in introductory provisions to reflect the probable intent of Congress.

Subsec. (c). Pub. L. 108-458, §1072(d)(1)(A), which directed amendment of subsec. (c) by substituting “section 403-1(i)” for “section 403-3(c)(6)”, was executed by making the substitution for “section 403-3(c)(7)” to reflect the probable intent of Congress and the amendment by Pub. L. 108-177. See 2003 Amendment note below.

2003—Subsecs. (c), (e)(2). Pub. L. 108-177, §377(d), substituted “section 403-3(c)(7) of this title” for “section 403-3(c)(6) of this title”.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108-458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108-458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

¹ See References in Text note below.

§ 3364. Assignment of responsibilities relating to analytic integrity

(a) Assignment of responsibilities

For purposes of carrying out section 3024(h) of this title, the Director of National Intelligence shall, not later than 180 days after December 17, 2004, assign an individual or entity to be responsible for ensuring that finished intelligence products produced by any element or elements of the intelligence community are timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic tradecraft.

(b) Responsibilities

(1) The individual or entity assigned responsibility under subsection (a)—

(A) may be responsible for general oversight and management of analysis and production, but may not be directly responsible for, or involved in, the specific production of any finished intelligence product;

(B) shall perform, on a regular basis, detailed reviews of finished intelligence product or other analytic products by an element or elements of the intelligence community covering a particular topic or subject matter;

(C) shall be responsible for identifying on an annual basis functional or topical areas of analysis for specific review under subparagraph (B); and

(D) upon completion of any review under subparagraph (B), may draft lessons learned, identify best practices, or make recommendations for improvement to the analytic tradecraft employed in the production of the reviewed product or products.

(2) Each review under paragraph (1)(B) should—

(A) include whether the product or products concerned were based on all sources of available intelligence, properly describe the quality and reliability of underlying sources, properly caveat and express uncertainties or confidence in analytic judgments, properly distinguish between underlying intelligence and the assumptions and judgments of analysts, and incorporate, where appropriate, alternative analyses; and

(B) ensure that the analytic methodologies, tradecraft, and practices used by the element or elements concerned in the production of the product or products concerned meet the standards set forth in subsection (a).

(3) Information drafted under paragraph (1)(D) should, as appropriate, be included in analysis teaching modules and case studies for use throughout the intelligence community.

(c) Annual briefings

Not later than February 1 each year, the Director of National Intelligence shall provide to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a briefing with a description, and the associated findings, of each review under subsection (b)(1)(B) during such year.

(d) Congressional intelligence committees defined

In this section, the term “congressional intelligence committees” means—

(1) the Select Committee on Intelligence of the Senate; and

(2) the Permanent Select Committee on Intelligence of the House of Representatives.

(Pub. L. 108–458, title I, § 1019, Dec. 17, 2004, 118 Stat. 3671; Pub. L. 116–92, div. E, title LVII, § 5701(b), Dec. 20, 2019, 133 Stat. 2159; Pub. L. 118–159, div. F, title LXIX, § 6901(b), Dec. 23, 2024, 138 Stat. 2516.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403–1a of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2024—Subsec. (c). Pub. L. 118–159 substituted “February 1” for “December 1”.

2019—Subsec. (c). Pub. L. 116–92 substituted “briefings” for “reports” in heading and “provide to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a briefing with” for “submit to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a report containing” in text.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

For Determination by President that section take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108–458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

ANNUAL TRAINING REQUIREMENT AND REPORT REGARDING ANALYTIC STANDARDS

Pub. L. 117–263, div. F, title LXIII, § 6312, Dec. 23, 2022, 136 Stat. 3510, provided that:

“(a) **POLICY FOR TRAINING PROGRAM REQUIRED.**—Consistent with sections 1019 and 1020 of the Intelligence Reform and Terrorism Prevention Act of 2004 [Pub. L. 108–458] (50 U.S.C. 3364 and 3364 note), the Director of National Intelligence shall issue a policy that requires each head of an element of the intelligence community, that has not already done so, to create, before the date that is 180 days after the date of the enactment of this Act [Dec. 23, 2022], an annual training program on the standards set forth in Intelligence Community Directive 203, Analytic Standards (or successor directive).

“(b) **CONDUCT OF TRAINING.**—Training required pursuant to the policy required by subsection (a) may be conducted in conjunction with other required annual training programs conducted by the element of the intelligence community concerned.

“(c) **CERTIFICATION OF COMPLETION OF TRAINING.**—Each year, each head of an element of the intelligence community shall submit to the congressional intelligence committees a certification as to whether all of the analysts of that element have completed the training required pursuant to the policy required by subsection (a) and if the analysts have not, an explanation of why the training has not been completed.

“(d) **REPORTS.**—

“(1) ANNUAL REPORT.—In conjunction with each briefing provided under section 1019(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3364(c)), the Director shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report on the number and themes of compliance incidents reported to intelligence community analytic ombudspersons relating to the standards set forth in Intelligence Community Directive 203 (relating to analytic standards), or successor directive.

“(2) REPORT ON PERFORMANCE EVALUATION.—Not later than 90 days after the date of the enactment of this Act, the head of analysis at each element of the intelligence community that conducts all-source analysis shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report describing how compliance with the standards set forth in Intelligence Community Directive 203 (relating to analytic standards), or successor directive, is considered in the performance evaluations and consideration for merit pay, bonuses, promotions, and any other personnel actions for analysts within the element.

“(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prohibit the Director from providing training described in this section as a service of common concern.

“(f) SUNSET.—This section shall cease to be effective on the date that is 5 years after the date of the enactment of this Act [Dec. 23, 2022].”

[For definitions of “intelligence community” and “congressional intelligence committees” as used in section 6312 of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.]

SAFEGUARD OF OBJECTIVITY IN INTELLIGENCE ANALYSIS

Pub. L. 108–458, title I, §1020, Dec. 17, 2004, 118 Stat. 3672, provided that:

“(a) IN GENERAL.—Not later than 180 days after the effective date of this Act [probably means the effective date of title I of Pub. L. 108–458, see Effective Date of 2004 Amendment; Transition Provisions note set out under section 3001 of this title], the Director of National Intelligence shall identify an individual within the Office of the Director of National Intelligence who shall be available to analysts within the Office of the Director of National Intelligence to counsel, conduct arbitration, offer recommendations, and, as appropriate, initiate inquiries into real or perceived problems of analytic tradecraft or politicization, biased reporting, or lack of objectivity in intelligence analysis.

“(b) REPORT.—Not later than 270 days after the effective date of this Act, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives on the implementation of subsection (a).”

§ 3365. Foreign intelligence information

(1) In general

Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3003 of this title) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only

as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Consistent with the responsibility of the Director of Central Intelligence to protect intelligence sources and methods, and the responsibility of the Attorney General to protect sensitive law enforcement information, it shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

(2) Definition

In this section, the term “foreign intelligence information” means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(Pub. L. 107–56, title II, §203(d), Oct. 26, 2001, 115 Stat. 281; Pub. L. 107–296, title VIII, §897(a), Nov. 25, 2002, 116 Stat. 2257; Pub. L. 117–347, title III, §323(a)(1)(A), Jan. 5, 2023, 136 Stat. 6206.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403–5d of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2023—Par. (1). Pub. L. 117–347, §323(a)(1)(A), repealed Pub. L. 107–296, §897(a). See 2002 Amendment note below.

2002—Par. (1). Pub. L. 107-296, 897(a), which inserted at end “Consistent with the responsibility of the Director of Central Intelligence to protect intelligence sources and methods, and the responsibility of the Attorney General to protect sensitive law enforcement information, it shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.”, was repealed by Pub. L. 117-347, § 323(a)(1)(A). Repeal to have no effect on amendment by Pub. L. 107-296, see Construction of 2023 Amendment note set out under section 2517 of Title 18, Crimes and Criminal Procedure.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 3001 of this title.

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

§ 3366. Authorities of heads of other departments and agencies

Notwithstanding any other provision of law, the head of any department or agency of the United States is authorized to receive and utilize funds made available to the department or agency by the Director of National Intelligence pursuant to section 3024(d)(2) of this title, as amended by subsection (a), and receive and utilize any system referred to in such section that is made available to such department or agency.

(Pub. L. 111-259, title IV, § 402(b), Oct. 7, 2010, 124 Stat. 2709.)

Editorial Notes

REFERENCES IN TEXT

Subsection (a), referred to in text, is subsec. (a) of section 402 of Pub. L. 111-259, title IV, Oct. 7, 2010, 124 Stat. 2708, which amended section 403-1 of this title prior to editorial reclassification and renumbering as section 3024 of this title.

CODIFICATION

Section was formerly classified as a note under section 403-1 of this title prior to editorial reclassification as this section.

§ 3367. Requirement for efficient use by intelligence community of open-source intelligence

The Director of National Intelligence shall ensure that the intelligence community makes efficient and effective use of open-source information and analysis.

(Pub. L. 108-458, title I, § 1052(b), Dec. 17, 2004, 118 Stat. 3683.)

Editorial Notes

CODIFICATION

Section was formerly classified as a note under section 403-1 of this title prior to editorial reclassification as this section.

Statutory Notes and Related Subsidiaries

INTELLIGENCE COMMUNITY DIRECTIVE WITH RESPECT TO OPEN-SOURCE INTELLIGENCE

Pub. L. 118-31, div. G, title III, § 7321(d), (e), Dec. 22, 2023, 137 Stat. 1038, provided that:

“(d) INTELLIGENCE COMMUNITY DIRECTIVE WITH RESPECT TO OPEN-SOURCE INTELLIGENCE.—Not later than 180 days after the date of the enactment of this Act [Dec. 22, 2023], the Director of National Intelligence shall update Intelligence Community Directive 208, Maximizing the Utility of Analytic Products (or any successor directive) to specifically address—

“(1) the production and dissemination of unclassified intelligence products derived entirely from open-source intelligence, including from unclassified publicly available information, unclassified commercially available information, or any other type of unclassified information; and

“(2) the needs and requirements of covered individuals who do not hold a security clearance or have access to the classified systems on which such unclassified intelligence products reside.

“(e) DEFINITIONS.—In this section:

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

“(A) the congressional intelligence committees;

“(B) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Committee on Appropriations of the Senate; and

“(C) the Committee on Oversight and Accountability, the Committee on the Judiciary, and the Committee on Appropriations of the House of Representatives.

“(2) COVERED INDIVIDUAL.—The term ‘covered individual’ means an employee of the Federal Government—

“(A) who is not an employee or contractor of an element of the intelligence community; and

“(B) who would derive value from a covered open-source intelligence product.

“(3) COVERED OPEN-SOURCE INTELLIGENCE PRODUCT.—The term ‘covered open-source intelligence product’ means an unclassified product derived from open-source intelligence that is produced by the intelligence community.”

[For definitions of “intelligence community” and “congressional intelligence committees” as used in section 7321(d), (e) of Pub. L. 118-31, set out above, see sec-

tion 7002 of Pub. L. 118-31, set out as a note under section 3003 of this title.]

ASSESSING INTELLIGENCE COMMUNITY OPEN-SOURCE SUPPORT FOR EXPORT CONTROLS AND FOREIGN INVESTMENT SCREENING

Pub. L. 117-263, div. F, title LXIII, § 6311, Dec. 23, 2022, 136 Stat. 3508, provided that:

“(a) PILOT PROGRAM TO ASSESS OPEN SOURCE SUPPORT FOR EXPORT CONTROLS AND FOREIGN INVESTMENT SCREENING.—

“(1) PILOT PROGRAM AUTHORIZED.—The Director of National Intelligence shall designate an element of the intelligence community to carry out a pilot program to assess the feasibility and advisability of providing enhanced intelligence support, including intelligence derived from open source, publicly and commercially available information—

“(A) to the Department of Commerce to support the export control and investment screening functions of the Department; and

“(B) to the Department of Homeland Security to support the export control functions of the Department.

“(2) AUTHORITY.—In carrying out the pilot program required by paragraph (1), the element designated by the Director under such paragraph—

“(A) shall establish a process for the provision of information as described in such paragraph; and

“(B) may—

“(i) acquire and prepare data, consistent with applicable provisions of law and Executive orders;

“(ii) modernize analytic systems, including through the acquisition, development, or application of automated tools; and

“(iii) establish standards and policies regarding the acquisition, treatment, and sharing of open source, publicly and commercially available information.

“(3) DURATION.—The pilot program required by paragraph (1) shall be carried out during a 3-year period.

“(b) PLAN AND REPORT REQUIRED.—

“(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ‘appropriate committees of Congress’ means—

“(A) the Select Committee on Intelligence, the Committee on Banking, Housing, and Urban Affairs, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

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

“(2) PLAN.—

“(A) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2022], the Director shall, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, submit to the appropriate committees of Congress a plan to carry out the pilot program required by subsection (a)(1).

“(B) CONTENTS.—The plan submitted under subparagraph (A) shall include the following:

“(i) A list, developed in consultation with the Secretary of Commerce and the Secretary of Homeland Security, of the activities of the Department of Commerce and the Department of Homeland Security that will be supported by the pilot program.

“(ii) A plan for measuring the effectiveness of the pilot program and the value of open source, publicly and commercially available information to the export control and investment screening missions.

“(3) REPORT.—

“(A) IN GENERAL.—Not later than 540 days after the date on which the Director submits the plan

under paragraph (2)(A), the Director shall submit to the appropriate committees of Congress a report on the findings of the Director with respect to the pilot program.

“(B) CONTENTS.—The report submitted under subparagraph (A) shall include the following:

“(i) An assessment of the feasibility and advisability of providing information as described in subsection (a)(1).

“(ii) An assessment of the value of open source, publicly and commercially available information to the export control and investment screening missions, using the measures of effectiveness under paragraph (2)(B)(ii).

“(iii) Identification of opportunities for and barriers to more effective use of open source, publicly and commercially available information by the intelligence community.”

[For definition of “intelligence community” as used in section 6311 of Pub. L. 117-263, set out above, see section 6002 of Pub. L. 117-263, set out as a note under section 3003 of this title.]

§ 3368. Assistance for governmental entities and private entities in recognizing online violent extremist content

(a) Assistance to recognize online violent extremist content

Not later than 180 days after May 5, 2017, and consistent with the protection of intelligence sources and methods, the Director of National Intelligence shall publish on a publicly available Internet website a list of all logos, symbols, insignia, and other markings commonly associated with, or adopted by, an organization designated by the Secretary of State as a foreign terrorist organization under section 1189(a) of title 8.

(b) Updates

The Director shall update the list published under subsection (a) every 180 days until December 22, 2023.

(Pub. L. 115-31, div. N, title IV, § 403, May 5, 2017, 131 Stat. 820; Pub. L. 118-31, div. G, title III, § 7327(d), Dec. 22, 2023, 137 Stat. 1045.)

Editorial Notes

AMENDMENTS

2023—Subsec. (b). Pub. L. 118-31 substituted “until December 22, 2023” for “or more frequently as needed”.

§ 3369. Cooperative actions to detect and counter foreign influence operations

(a) Findings

Congress makes the following findings:

(1) The Russian Federation, through military intelligence units, also known as the “GRU”, and Kremlin-linked troll organizations often referred to as the “Internet Research Agency”, deploy information warfare operations against the United States, its allies and partners, with the goal of advancing the strategic interests of the Russian Federation.

(2) One line of effort deployed as part of these information warfare operations is the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion.

(3) These information warfare operations are a threat to the national security of the United States and that of the allies and partners of the United States. As former Director of National Intelligence Dan Coats stated, “These actions are persistent, they are pervasive and they are meant to undermine America’s democracy.”.

(4) These information warfare operations continue to evolve and increase in sophistication.

(5) Other foreign adversaries and hostile non-state actors are increasingly adopting similar tactics of deploying information warfare operations against the West, such as recent state-backed operations from China around the Hong Kong protests identified by social media companies.

(6) Technological advances, including artificial intelligence, will only make it more difficult in the future to detect fraudulent accounts, deceptive material posted on social media, and malign behavior on social media platforms.

(7) Because these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms.

(8) The social media companies are inherently technologically sophisticated and adept at rapidly analyzing large amounts of data and developing software-based solutions to diverse and ever-changing challenges on their platforms, which makes them well-equipped to address the threat occurring on their platforms.

(9) Independent analyses confirmed Kremlin-linked threat networks, based on data provided by several social media companies to the Select Committee on Intelligence of the Senate, thereby demonstrating that it is possible to discern both broad patterns of cross-platform information warfare operations and specific fraudulent behavior on social media platforms.

(10) General Paul Nakasone, Director of the National Security Agency, emphasized the importance of these independent analyses to the planning and conducting of military cyber operations to frustrate Kremlin-linked information warfare operations against the 2018 mid-term elections. General Nakasone stated that the reports “were very, very helpful in terms of being able to understand exactly what our adversary was trying to do to build dissent within our nation.”.

(11) Institutionalizing ongoing robust, independent, and vigorous analysis of data related to foreign threat networks within and across social media platforms will help counter ongoing information warfare operations against the United States, its allies, and its partners.

(12) Archiving and disclosing to the public the results of these analyses by the social media companies and trusted third-party experts in a transparent manner will serve to demonstrate that the social media companies are detecting and removing foreign malign activities from their platforms while protecting

the privacy of the people of the United States and will build public understanding of the scale and scope of these foreign threats to our democracy, since exposure is one of the most effective means to build resilience.

(b) Sense of Congress

It is the sense of Congress that—

(1) the social media companies should cooperate among themselves and with independent organizations and researchers on a sustained and regular basis to share and analyze data and indicators relevant to foreign information warfare operations within and across their platforms in order to detect and counter foreign information warfare operations that threaten the national security of the United States and its allies and partners;

(2) information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations;

(3) these analytic efforts should be organized in such a fashion as to meet the highest standards of ethics, confidentiality, and privacy protection of the people of the United States, while still allowing timely research access to relevant data;

(4) these analytic efforts should be undertaken as soon as possible to facilitate countering ongoing state or state-backed foreign information warfare operations and to aid in preparations for the United States Presidential and congressional elections in 2020 and beyond;

(5) the structure and operations of social media companies make them well positioned to work with independent organizations and researchers to address foreign adversary threat networks within and across their platforms, and these efforts could be conducted without direct Government involvement, direction, or regulation; and

(6) if the social media industry fails to take sufficient action to address foreign adversary threat networks operating within or across their platforms, Congress would have to consider additional safeguards for ensuring that this threat is effectively mitigated.

(c) Requirement to facilitate establishment of Social Media Data and Threat Analysis Center

(1) Requirement

Not later than June 1, 2021, the Director of National Intelligence, in coordination with the Secretary of Defense, shall facilitate, by grant or contract or under an existing authority of the Director, the establishment of a Social Media Data and Threat Analysis Center with the functions described in paragraph (2) at an independent, nonprofit organization.

(2) Functions

The functions described in this paragraph are the following:

(A) Acting as a convening and sponsoring authority for cooperative social media data analysis of foreign threat networks involving social media companies and third-party experts, nongovernmental organizations, data journalists, Federally funded research

and development centers, academic researchers, traditional media, and international counterparts, as appropriate.

(B) Facilitating analysis of foreign influence operation, within and across the individual social media platforms as well as hacking and leaking campaigns, and other tactics, and related unlawful activities that fund or subsidize such operations.

(C) Developing processes to share information from government entities on foreign influence operations with the individual social media companies to inform threat analysis, and working with the Office of the Director of National Intelligence as appropriate.

(D) Determining and making public criteria for identifying which companies, organizations, or researchers qualify for inclusion in the activities of the Center, and inviting entities that fit the criteria to join.

(E) Determining jointly with the social media companies what data and metadata related to indicators of foreign adversary threat networks from their platforms and business operations will be made available for access and analysis.

(F) Developing and making public the criteria and standards that must be met for companies, other organizations, and individual researchers to access and analyze data relating to foreign adversary threat networks within and across social media platforms and publish or otherwise use the results.

(G) Developing and making public the ethical standards for investigation of foreign threat networks and use of analytic results and for protection of the privacy of the customers and users of the social media platforms and of the proprietary information of the social media companies.

(H) Developing technical, contractual, and procedural controls to prevent misuse of data, including any necessary auditing procedures, compliance checks, and review mechanisms.

(I) Developing and making public criteria and conditions under which the Center shall share information with the appropriate Government agencies regarding threats to national security from, or violations of the law involving, foreign activities on social media platforms.

(J) Hosting a searchable archive aggregating information related to foreign influence and disinformation operations to build a collective understanding of the threats and facilitate future examination consistent with privacy protections.

(K) Developing data standards to harmonize the sharing of information pursuant to this paragraph.

(d) Reporting and notifications

The Director of the Center shall—

(1) not later than August 1, 2021, submit to appropriate congressional committees a report on—

(A) the estimated funding needs of the Center for fiscal year 2021 and for subsequent years;

(B) such statutory protections from liability as the Director considers necessary for the Center, participating social media companies, and participating third-party analytical participants;

(C) such statutory penalties as the Director considers necessary to ensure against misuse of data by researchers; and

(D) such changes to the Center's mission to fully capture broader unlawful activities that intersect with, complement, or support information warfare tactics; and

(2) not less frequently than once each year, submit to the Director of National Intelligence, the Secretary of Defense, and the appropriate congressional committees a report—

(A) that assesses—

(i) degree of cooperation and commitment from the social media companies to the mission of the Center; and

(ii) effectiveness of the Center in detecting and facilitating the removal or neutralization of clandestine foreign information warfare operations from social media platforms; and

(B) includes such recommendations for legislative or administrative action as the Center considers appropriate to carry out the functions of the Center.

(e) Periodic reporting to the public

The Director of the Center shall—

(1) once each quarter, make available to the public a report on key trends in foreign influence and disinformation operations, including any threats to campaigns and elections, to inform the public of the United States; and

(2) as the Director considers necessary, provide more timely assessments relating to ongoing disinformation campaigns.

(f) Foreign malign influence campaigns on social media platforms targeting elections for Federal office

(1) Reports

(A) Requirement

Not later than 90 days before the date of each regularly scheduled general election for Federal office, the Director of the Center shall submit to the appropriate congressional committees a report on foreign malign influence campaigns on and across social media platforms targeting such election.

(B) Matters included

Each report under subparagraph (A) shall include an analysis of the following:

(i) The patterns, tools, and techniques of foreign malign influence campaigns across all platforms on social media by a covered foreign country targeting a regularly scheduled general election for Federal office.

(ii) Inauthentic accounts and “bot” networks across platforms, including the scale to which such accounts or networks exist, how platforms currently act to remove such accounts or networks, and what percentage of such accounts or networks

have been removed during the period covered by the report.

(iii) The estimated reach and impact of intentional or weaponized disinformation by inauthentic accounts and “bot” networks, including an analysis of amplification by users and algorithmic distribution.

(iv) The trends of types of media that are being used for dissemination through foreign malign influence campaigns, including machine-manipulated media, and the intended targeted groups.

(C) Initial report

Not later than August 1, 2021, the Director of the Center shall submit to the appropriate congressional committees a report under subparagraph (A) addressing the regularly scheduled general election for Federal office occurring during 2020.

(D) Form

Each report under this paragraph shall be submitted in an unclassified form, but may include a classified annex.

(2) Briefings

(A) Requirement

Not later than 30 days after the date on which the Director submits to the appropriate congressional committees a report under paragraph (1), the Director of National Intelligence, in coordination with the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, shall provide to such committees a briefing assessing threats from foreign malign influence campaigns on social media from covered countries to the regularly scheduled general election for Federal office covered by the report.

(B) Matters to be included

Each briefing under subparagraph (A) shall include the following:

(i) The patterns, tools, and techniques of foreign malign influence campaigns across all platforms on social media by a covered foreign country targeting a regularly scheduled general election for Federal office.

(ii) An assessment of the findings from the report for which the briefing is provided.

(iii) The activities and methods used to mitigate the threats associated with such findings by the Department of Defense, the Department of Homeland Security, or other relevant departments or agencies of the Federal Government.

(iv) The steps taken by departments or agencies of the Federal Government to cooperate with social media companies to mitigate the threats identified.

(g) Funding

Of the amounts appropriated or otherwise made available to the National Intelligence Program (as defined in section 3003 of this title) in fiscal year 2021 and 2022, the Director of National Intelligence may use up to \$30,000,000 to carry out this section.

(h) Definitions

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

(A) the congressional intelligence committees;

(B) the Committee on Armed Services, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives; and

(C) the Committee on Armed Services, the Committee on Appropriations, the Committee on Homeland Security and Government Affairs, the Committee on Foreign Relations, and the Committee on the Judiciary of the Senate.

(2) Covered foreign country and foreign malign influence

The terms “covered foreign country” and “foreign malign influence” have the meanings given those terms in section 3059 of this title.

(3) Machine-manipulated media

The term “machine-manipulated media” has the meaning given that term in section 5724.¹

(Pub. L. 116–92, div. E, title LIII, § 5323, Dec. 20, 2019, 133 Stat. 2130; Pub. L. 116–283, div. H, title XCIII, § 9301, Jan. 1, 2021, 134 Stat. 4801.)

Editorial Notes

REFERENCES IN TEXT

Section 5724, referred to in subsec. (h)(3), is section 5724 of Pub. L. 116–92, which is set out as a note under section 3024 of this title.

AMENDMENTS

2021—Pub. L. 116–283, § 9301(d)(3)(A), struck out “Encouragement of” before “Cooperative” in section catchline.

Subsec. (c). Pub. L. 116–283, § 9301(d)(3)(B)(i), substituted “Requirement” for “Authority” in heading.

Subsec. (c)(1). Pub. L. 116–283, § 9301(a), (d)(3)(B)(ii), in heading, substituted “Requirement” for “Authority” and, in text, substituted “Not later than June 1, 2021, the Director” for “The Director” and “shall” for “may”.

Subsec. (d). Pub. L. 116–283, § 9301(d)(1)(A), substituted “The” for “If the Director of National Intelligence chooses to use funds under subsection (c)(1) to facilitate the establishment of the Center, the” in introductory provisions.

Subsec. (d)(1). Pub. L. 116–283, § 9301(d)(1)(B), substituted “August 1, 2021” for “180 days after December 20, 2019”.

Subsec. (f). Pub. L. 116–283, § 9301(b)(2), added subsec. (f). Former subsec. (f) redesignated (g).

Subsec. (g). Pub. L. 116–283, § 9301(d)(2), substituted “fiscal year 2021 and 2022” for “fiscal year 2020 and 2021”.

Pub. L. 116–283, § 9301(b)(1), redesignated subsec. (f) as (g). Former subsec. (g) redesignated (h).

Subsec. (h). Pub. L. 116–283, § 9301(c), amended subsec. (h) generally. Prior to amendment, subsec. (h) defined “appropriate congressional committees”.

Pub. L. 116–283, § 9301(b)(1), redesignated subsec. (g) as (h).

¹ See References in Text note below.

Statutory Notes and Related Subsidiaries**DEFINITIONS**

For definition of “intelligence community”, referred to subsec. (b)(2), see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3369a. Report on deepfake technology, foreign weaponization of deepfakes, and related notifications

(a) Report on foreign weaponization of deepfakes and deepfake technology

(1) Report required

Not later than 180 days after December 20, 2019, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined appropriate by the Director, shall submit to the congressional intelligence committees a report on—

(A) the potential national security impacts of machine-manipulated media (commonly known as “deepfakes”); and

(B) the actual or potential use of machine-manipulated media by foreign governments to spread disinformation or engage in other malign activities.

(2) Matters to be included

The report under subsection (a) shall include the following:

(A) An assessment of the technical capabilities of foreign governments, including foreign intelligence services, foreign government-affiliated entities, and foreign individuals, with respect to machine-manipulated media, machine-generated text, generative adversarial networks, and related machine-learning technologies, including—

(i) an assessment of the technical capabilities of the People’s Republic of China and the Russian Federation with respect to the production and detection of machine-manipulated media; and

(ii) an annex describing those governmental elements within China and Russia known to have supported or facilitated machine-manipulated media research, development, or dissemination, as well as any civil-military fusion, private-sector, academic, or nongovernmental entities which have meaningfully participated in such activities.

(B) An updated assessment of how foreign governments, including foreign intelligence services, foreign government-affiliated entities, and foreign individuals, could use or are using machine-manipulated media and machine-generated text to harm the national security interests of the United States, including an assessment of the historic, current, or potential future efforts of China and Russia to use machine-manipulated media, including with respect to—

(i) the overseas or domestic dissemination of misinformation;

(ii) the attempted discrediting of political opponents or disfavored populations; and

(iii) intelligence or influence operations directed against the United States, allies

or partners of the United States, or other jurisdictions believed to be subject to Chinese or Russian interference.

(C) An updated identification of the countertechnologies that have been or could be developed and deployed by the United States Government, or by the private sector with Government support, to deter, detect, and attribute the use of machine-manipulated media and machine-generated text by foreign governments, foreign-government affiliates, or foreign individuals, along with an analysis of the benefits, limitations and drawbacks of such identified countertechnologies, including any emerging concerns related to privacy.

(D) An identification of the offices within the elements of the intelligence community that have, or should have, lead responsibility for monitoring the development of, use of, and response to machine-manipulated media and machine-generated text, including—

(i) a description of the coordination of such efforts across the intelligence community;

(ii) a detailed description of the existing capabilities, tools, and relevant expertise of such elements to determine whether a piece of media has been machine manipulated or machine generated, including the speed at which such determination can be made, the confidence level of the element in the ability to make such a determination accurately, and how increasing volume and improved quality of machine-manipulated media or machine-generated text may negatively impact such capabilities; and

(iii) a detailed description of planned or ongoing research and development efforts intended to improve the ability of the intelligence community to detect machine-manipulated media and machine-generated text.

(E) A description of any research and development activities carried out or under consideration to be carried out by the intelligence community, including the Intelligence Advanced Research Projects Activity, relevant to machine-manipulated media and machine-generated text detection technologies.

(F) Updated recommendations regarding whether the intelligence community requires additional legal authorities, financial resources, or specialized personnel to address the national security threat posed by machine-manipulated media and machine-generated text.

(G) Other additional information the Director determines appropriate.

(b) Form

The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) Requirement for notification

The Director of National Intelligence, in cooperation with the heads of any other relevant

departments or agencies of the Federal Government, shall notify the congressional intelligence committees each time the Director of National Intelligence determines—

(1) there is credible information or intelligence that a foreign entity has attempted, is attempting, or will attempt to deploy machine-manipulated media or machine-generated text aimed at the elections or domestic political processes of the United States; and

(2) that such intrusion or campaign can be attributed to a foreign government, a foreign government-affiliated entity, or a foreign individual.

(d) Definitions

(1) Machine-generated text

The term “machine-generated text” means text generated using machine-learning techniques in order to resemble writing in natural language.

(2) Machine-manipulated media

The term “machine-manipulated media” has the meaning given that term in section 5724.¹

(Pub. L. 116-92, div. E, title LVII, § 5709, Dec. 20, 2019, 133 Stat. 2168; Pub. L. 117-263, div. F, title LXVIII, § 6811(b), Dec. 23, 2022, 136 Stat. 3600.)

Editorial Notes

REFERENCES IN TEXT

Section 5724, referred to in subsec. (d)(2), means section 5724 of Pub. L. 116-92, which is set out as a note under section 3024 of this title.

AMENDMENTS

2022—Subsecs. (d), (e). Pub. L. 117-263 redesignated subsec. (e) as (d) and struck out former subsec. (d). Prior to amendment, text of subsec. (d) read as follows: “Upon submission of the report in subsection (a), on an annual basis, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined appropriate by the Director, shall submit to the congressional intelligence committees any significant updates with respect to the matters described in subsection (a).”

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3369b. Oversight of foreign influence in academia

(a) Definitions

In this section:

(1) Covered institution of higher education

The term “covered institution of higher education” means an institution described in section 1002 of title 20 that receives Federal funds in any amount and for any purpose.

(2) Sensitive research subject

The term “sensitive research subject” means a subject of research that is carried out at a covered institution of higher education

that receives funds that were appropriated for—

(A) the National Intelligence Program; or

(B) any Federal agency the Director of National Intelligence deems appropriate.

(b) Report required

Not later than 180 days after December 20, 2019, and not less frequently than once each year thereafter, the Director of National Intelligence, in consultation with such elements of the intelligence community as the Director considers appropriate and consistent with the privacy protections afforded to United States persons, shall provide to congressional intelligence committees a briefing on risks to sensitive research subjects posed by foreign entities in order to provide Congress and covered institutions of higher education with more complete information on these risks and to help ensure academic freedom.

(c) Contents

The briefing required by subsection (b) shall include the following:

(1) A list of sensitive research subjects that could affect national security.

(2) A list of foreign entities, including governments, corporations, nonprofit organizations and for-profit organizations, and any subsidiary or affiliate of such an entity, that the Director determines pose a counterintelligence, espionage (including economic espionage), or other national security threat with respect to sensitive research subjects.

(3) A list of any known or suspected attempts by foreign entities to exert pressure on covered institutions of higher education, including attempts to limit freedom of speech, propagate misinformation or disinformation, or to influence professors, researchers, or students.

(4) Recommendations for collaboration between covered institutions of higher education and the intelligence community to mitigate threats to sensitive research subjects associated with foreign influence in academia, including any necessary legislative or administrative action.

(d) Congressional notifications required

Not later than 30 days after the date on which the Director identifies a change to either list described in paragraph (1) or (2) of subsection (c), the Director shall notify the congressional intelligence committees of the change.

(Pub. L. 116-92, div. E, title LVII, § 5713, Dec. 20, 2019, 133 Stat. 2172; Pub. L. 118-159, div. F, title LXIX, § 6901(c), Dec. 23, 2024, 138 Stat. 2516.)

Editorial Notes

AMENDMENTS

2024—Subsec. (b). Pub. L. 118-159, § 6901(c)(1), substituted “shall provide” for “shall submit” and “briefing” for “report”. “Report” in subsec. heading was not amended.

Subsec. (c). Pub. L. 118-159, § 6901(c)(2), substituted “briefing” for “report” in introductory provisions.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in

¹ See References in Text note below.

this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3369c. Notification of an active measures campaign

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

- (A) the congressional intelligence committees;
- (B) the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and
- (C) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) Congressional leadership

The term “congressional leadership” includes the following:

- (A) The majority leader of the Senate.
- (B) The minority leader of the Senate.
- (C) The Speaker of the House of Representatives.
- (D) The minority leader of the House of Representatives.

(b) Requirement for notification

The Director of National Intelligence, in cooperation with the Director of the Federal Bureau of Investigation and the head of any other relevant agency, shall notify the congressional leadership and the chairman and vice chairman or ranking member of each of the appropriate congressional committees, and of other relevant committees of jurisdiction, each time the Director of National Intelligence determines there is credible information that a foreign power has, is, or will attempt to employ a covert influence or active measures campaign with regard to the modernization, employment, doctrine, or force posture of the nuclear deterrent or missile defense.

(c) Content of notification

Each notification required by subsection (b) shall include information concerning actions taken by the United States to expose or halt an attempt referred to in subsection (b).

(Pub. L. 116-92, div. E, title LXVII, § 6703, Dec. 20, 2019, 133 Stat. 2223.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3369d. Committee to counter active measures by the Russian Federation, the People’s Republic of China, the Islamic Republic of Iran, the Democratic People’s Republic of Korea, or other nation state to exert covert influence over peoples and governments

(a) Definitions

In this section:

(1) Active measures by Russia, China, Iran, North Korea, or other nation state to exert covert influence

The term “active measures by Russia, China, Iran, North Korea, or other nation state to exert covert influence” means activities intended to influence a person or government that are carried out in coordination with, or at the behest of, political leaders or the security services of the Russian Federation, the People’s Republic of China, the Islamic Republic of Iran, the Democratic People’s Republic of Korea, or other nation state and the role of the Russian Federation, the People’s Republic of China, the Islamic Republic of Iran, the Democratic People’s Republic of Korea, or other nation state has been hidden or not acknowledged publicly, including the following:

- (A) Establishment or funding of a front group.
- (B) Covert broadcasting.
- (C) Media manipulation.
- (D) Disinformation and forgeries.
- (E) Funding agents of influence.
- (F) Incitement and offensive counterintelligence.
- (G) Assassinations.
- (H) Terrorist acts.

(2) Appropriate committees of Congress

The term “appropriate committees of Congress” means—

- (A) the congressional intelligence committees;
- (B) the Committee on Armed Services and the Committee on Foreign Relations of the Senate; and
- (C) the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives.

(b) Establishment

There is established within the executive branch an interagency committee to counter active measures by the Russian Federation, the People’s Republic of China, the Islamic Republic of Iran, the Democratic People’s Republic of Korea, or other nation state to exert covert influence.

(c) Membership

(1) In general

(A) Appointment

Each head of an agency or department of the Government set out under subparagraph (B) shall appoint one member of the committee established by subsection (b) from among officials of such agency or department who occupy a position that is required to be appointed by the President, with the advice and consent of the Senate.

(B) Head of an agency or department

The head of an agency or department of the Government set out under this subparagraph are the following:

- (i) The Director of National Intelligence.
- (ii) The Secretary of State.
- (iii) The Secretary of Defense.
- (iv) The Secretary of the Treasury.

- (v) The Attorney General.
- (vi) The Secretary of Energy.
- (vii) The Director of the Federal Bureau of Investigation.
- (viii) The head of any other agency or department of the United States Government designated by the President for purposes of this section.

(d) Meetings

The committee shall meet on a regular basis.

(e) Duties

The duties of the committee established by subsection (b) shall be as follows:

- (1) To counter active measures by Russia, China, Iran, North Korea, or other nation state to exert covert influence, including by exposing falsehoods, agents of influence, corruption, human rights abuses, terrorism, and assassinations carried out by the security services or political elites of the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state or their proxies.
- (2) Such other duties as the President may designate for purposes of this section.

(f) Staff

The committee established by subsection (b) may employ such staff as the members of such committee consider appropriate.

(g) Budget Request

A request for funds required for the functioning of the committee established by subsection (b) may be included in each budget for a fiscal year submitted by the President pursuant to section 1105(a) of title 31.

(h) Annual report

(1) Requirement

Not later than 180 days after May 5, 2017, and annually thereafter, and consistent with the protection of intelligence sources and methods, the committee established by subsection (b) shall submit to the appropriate committees of Congress a report describing steps being taken by the committee to counter active measures by Russia, China, Iran, North Korea, or other nation state to exert covert influence.

(2) Content

Each report required by paragraph (1) shall include the following:

- (A) A summary of the active measures by the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state to exert covert influence during the previous year, including significant incidents and notable trends.
- (B) A description of the key initiatives of the committee.
- (C) A description of the implementation of the committee's initiatives by the head of an agency or department of the Government set out under subsection (c)(1)(B).
- (D) An analysis of the impact of the committee's initiatives.
- (E) Recommendations for changes to the committee's initiatives from the previous year.

(3) Separate reporting requirement

The requirement to submit an annual report under paragraph (1) is in addition to any other reporting requirements with respect to Russia, China, Iran, North Korea, or other nation state.

(Pub. L. 115–31, div. N, title V, § 501, May 5, 2017, 131 Stat. 823; Pub. L. 116–92, div. E, title LXVII, § 6706(a), Dec. 20, 2019, 133 Stat. 2224.)

Editorial Notes

CODIFICATION

Section was formerly set out as a note under section 3001 of this title.

AMENDMENTS

2019—Pub. L. 116–92, § 6706(a)(2), inserted “, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state” after “Russian Federation” in section catchline.

Pub. L. 116–92, § 6706(a)(1), wherever appearing, inserted “, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state” after “Russian Federation” and “, China, Iran, North Korea, or other nation state” after “Russia”.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3370. Supply Chain and Counterintelligence Risk Management Task Force

(a) Appropriate congressional committees defined

In this section, the term “appropriate congressional committees” means the following:

- (1) The congressional intelligence committees.
- (2) The Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate.
- (3) The Committee on Armed Services, the Committee on Homeland Security, and the Committee on Oversight and Reform of the House of Representatives.

(b) Requirement to establish

The Director of National Intelligence shall establish a Supply Chain and Counterintelligence Risk Management Task Force to standardize information sharing between the intelligence community and the acquisition community of the United States Government with respect to the supply chain and counterintelligence risks.

(c) Members

The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall be composed of—

- (1) a representative of the Defense Security Service of the Department of Defense;
- (2) a representative of the General Services Administration;
- (3) a representative of the Office of Federal Procurement Policy of the Office of Management and Budget;

- (4) a representative of the Department of Homeland Security;
- (5) a representative of the Federal Bureau of Investigation;
- (6) the Director of the National Counterintelligence and Security Center; and
- (7) any other members the Director of National Intelligence determines appropriate.

(d) Security clearances

Each member of the Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall have a security clearance at the top secret level and be able to access sensitive compartmented information.

(e) Annual report

The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall submit to the appropriate congressional committees an annual report that describes the activities of the Task Force during the previous year, including identification of the supply chain, cybersecurity, and counterintelligence risks shared with the acquisition community of the United States Government by the intelligence community.

(Pub. L. 116-92, div. E, title LXIII, § 6306, Dec. 20, 2019, 133 Stat. 2188.)

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

DEFINITIONS

For definitions of “congressional intelligence committees” and “intelligence community” as used in this section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3370a. Repealed. Pub. L. 118-159, div. F, title LXIX, § 6901(d), Dec. 23, 2024, 138 Stat. 2517

Section, Pub. L. 116-92, div. E, title LXVII, § 6716, Dec. 20, 2019, 133 Stat. 2227, related to a biennial report on foreign investment risks.

§ 3370b. Collaboration between intelligence community and Department of Commerce to counter foreign commercial threats

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

- (A) the congressional intelligence committees;
- (B) the Committee on Commerce, Science, and Transportation, the Committee on Armed Services, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and
- (C) the Committee on Energy and Commerce, the Committee on Armed Services, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(2) Foreign commercial threat

(A) In general

The term “foreign commercial threat” means a rare commercial item or service that is produced by, offered by, sold by, licensed by, or otherwise distributed under the control of a strategic competitor or foreign adversary in a manner that may provide the strategic competitor or foreign adversary leverage over an intended recipient.

(B) Determinations by Working Group

In determining whether an item or service is a foreign commercial threat, the Working Group shall consider whether the strategic competitor or foreign adversary could—

- (i) withhold, or threaten to withhold, the rare commercial item or service;
- (ii) create reliance on the rare commercial item or service as essential to the safety, health, or economic wellbeing of the intended recipient; or
- (iii) have its rare commercial item or service easily replaced by a United States entity or an entity of an ally or partner of the United States.

(3) Rare commercial item or service

The term “rare commercial item or service” means a good, service, or intellectual property that is not widely available for distribution.

(b) Working Group

(1) Establishment

Unless the Director of National Intelligence and the Secretary of Commerce make the joint determination specified in subsection (c), the Director and the Secretary, in consultation with the Secretary of State, shall jointly establish a working group to counter foreign commercial threats (in this section referred to as the “Working Group”).

(2) Membership

The composition of the Working Group may include any officer or employee of a department or agency of the United States Government determined appropriate by the Director or the Secretary.

(3) Duties

The duties of the Working Group shall be the following:

- (A) To identify current foreign commercial threats.
- (B) To identify probable future foreign commercial threats.
- (C) To identify goods, services, or intellectual property that, if produced by entities within the United States, or allies or partners of the United States, would mitigate foreign commercial threats.

(4) Meetings

Not later than 30 days after December 23, 2022, and on a regular basis that is not less frequently than quarterly thereafter until the date of termination under paragraph (5), the Working Group shall meet.

(5) Termination

Beginning on the date that is 2 years after the date of the establishment under paragraph

(1), the Working Group may be terminated upon the Director of National Intelligence and the Secretary of Commerce jointly—

(A) determining that termination of the Working Group is appropriate; and

(B) submitting to the appropriate congressional committees a notification of such determination (including a description of the justification for such determination).

(6) Reports

(A) Submission to Congress

Not later than 60 days after December 23, 2022, and biannually thereafter until the date of termination under paragraph (5), the Working Group shall submit to the appropriate congressional committees a report on the activities of the Working Group.

(B) Matters

Each report under subparagraph (A) shall include a description of the following:

(i) Any current or future foreign commercial threats identified by the Working Group.

(ii) The strategy of the United States Government, if any, to mitigate any current foreign commercial threats so identified.

(iii) The plan of the intelligence community to provide to the Department of Commerce and other nontraditional customers of the intelligence community support in addressing foreign commercial threats.

(iv) Any other significant activity of the Working Group.

(c) Option to discharge obligation through other means

If the Director of National Intelligence and the Secretary of Commerce make a joint determination that the requirements of the Working Group under subsection (b) (including the duties under paragraph (3) and the reporting requirement under paragraph (6) of such subsection) may be appropriately filled by an existing entity or structure, and submit to the congressional intelligence committees a notification of such determination (including a description of the justification for such determination), the Director and Secretary may task such entity or structure with such requirements in lieu of establishing the Working Group.

(Pub. L. 117–263, div. F, title LXV, § 6514, Dec. 23, 2022, 136 Stat. 3546.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.

§ 3371. Required counterintelligence assessments, briefings, notifications, and reports

(a) Foreign counterintelligence and cybersecurity threats to Federal election campaigns

(1) Reports required

(A) In general

As provided in subparagraph (B), with respect to an election for Federal office, the

Director of National Intelligence, in coordination with the Under Secretary of Homeland Security for Intelligence and Analysis and the Director of the Federal Bureau of Investigation, shall make publicly available on an internet website an advisory report on foreign counterintelligence and cybersecurity threats to campaigns of candidates for Federal office. Each such report, consistent with the protection of sources and methods, shall include the following:

(i) A description of foreign counterintelligence and cybersecurity threats to campaigns of candidates for Federal office.

(ii) A summary of best practices that campaigns of candidates for Federal office can employ in seeking to counter such threats.

(iii) An identification of publicly available resources, including United States Government resources, for countering such threats.

(B) Schedule for submittal

(i) In general

Except as provided by clause (ii), with respect to an election for Federal office, a report under this subsection shall be first made available not later than the date that is 1 year before the date of such election, and may be subsequently revised as the Director of National Intelligence determines appropriate.

(ii) 2020 elections

With respect to an election for Federal office that occurs during 2020, the report under this subsection shall be first made available not later than the date that is 60 days after December 20, 2020, and may be subsequently revised as the Director of National Intelligence determines appropriate.

(C) Information to be included

A report under this subsection shall reflect the most current information available to the Director of National Intelligence regarding foreign counterintelligence and cybersecurity threats.

(2) Treatment of campaigns subject to heightened threats

If the Director of the Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis jointly determine that a campaign of a candidate for Federal office is subject to a heightened foreign counterintelligence or cybersecurity threat, the Director and the Under Secretary, consistent with the protection of sources and methods, may make available additional information to the appropriate representatives of such campaign.

(b) Omitted

(c) Director of National Intelligence assessment of foreign interference in Federal elections

(1) Assessments required

Not later than 45 days after the end of a Federal election cycle, the Director of National Intelligence, in consultation with the heads of

such other executive departments and agencies as the Director considers appropriate, shall—

(A) conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in elections for Federal office occurring during the Federal election cycle; and

(B) transmit the findings of the Director with respect to the assessment conducted under subparagraph (A), along with such supporting information as the Director considers appropriate, to the following:

- (i) The President.
- (ii) The Secretary of State.
- (iii) The Secretary of the Treasury.
- (iv) The Secretary of Defense.
- (v) The Attorney General.
- (vi) The Secretary of Homeland Security.
- (vii) Congress.

(2) Elements

An assessment conducted under paragraph (1)(A), with respect to an act described in such paragraph, shall identify, to the maximum extent ascertainable, the following:

- (A) The nature of any foreign interference and any methods employed to execute the act.
- (B) The persons involved.
- (C) The foreign government or governments that authorized, directed, sponsored, or supported the act.

(3) Publication

The Director shall, not later than 60 days after the end of a Federal election cycle, make available to the public, to the greatest extent possible consistent with the protection of sources and methods, the findings transmitted under paragraph (1)(B).

(4) Federal election cycle defined

In this section, the term “Federal election cycle” means the period which begins on the day after the date of a regularly scheduled general election for Federal office and which ends on the date of the first regularly scheduled general election for Federal office held after such date.

(5) Effective date

This subsection shall apply with respect to the Federal election cycle that began during November 2018, and each succeeding Federal election cycle.

(Pub. L. 116–92, div. E, title LIII, § 5304, Dec. 20, 2019, 133 Stat. 2119.)

Editorial Notes

CODIFICATION

Section is comprised of section 5304 of Pub. L. 116–92. Subsec. (b) of section 5304 of Pub. L. 116–92 enacted section 3111 of this title and amended the analysis for the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

§ 3371a. Assessment of foreign intelligence threats to Federal elections

(a) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means—

- (A) the congressional intelligence committees;
- (B) the Committee on Homeland Security and Governmental Affairs of the Senate; and
- (C) the Committee on Homeland Security of the House of Representatives.

(2) Congressional leadership

The term “congressional leadership” includes the following:

- (A) The majority leader of the Senate.
- (B) The minority leader of the Senate.
- (C) The Speaker of the House of Representatives.
- (D) The minority leader of the House of Representatives.

(3) Security vulnerability

The term “security vulnerability” has the meaning given such term in section 650 of title 6.

(b) In general

The Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Director of the Federal Bureau of Investigation, the Secretary of Homeland Security, and the heads of other relevant elements of the intelligence community, shall—

- (1) commence not later than 1 year before any regularly scheduled Federal election occurring after December 31, 2018, and complete not later than 180 days before such election, an assessment of security vulnerabilities of State election systems; and
- (2) not later than 180 days before any regularly scheduled Federal election occurring after December 31, 2018, submit a report on such security vulnerabilities and an assessment of foreign intelligence threats to the election to—
 - (A) congressional leadership; and
 - (B) the appropriate congressional committees.

(c) Update

Not later than 90 days before any regularly scheduled Federal election occurring after December 31, 2018, the Director of National Intelligence shall—

- (1) update the assessment of foreign intelligence threats to that election; and
- (2) submit the updated assessment to—
 - (A) congressional leadership; and
 - (B) the appropriate congressional committees.

(Pub. L. 116–92, div. E, title LXV, § 6503, Dec. 20, 2019, 133 Stat. 2203; Pub. L. 117–263, div. G, title LXXI, § 7143(d)(7), Dec. 23, 2022, 136 Stat. 3664.)

Editorial Notes

AMENDMENTS

2022—Subsec. (a)(3). Pub. L. 117–263 substituted “section 650 of title 6” for “section 1501 of title 6”.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “congressional intelligence committees” and “intelligence community” as used in this

section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3371b. Information sharing with State election officials

(a) State defined

In this section, the term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(b) Security clearances

(1) In general

Not later than 30 days after December 20, 2019, the Director of National Intelligence shall support the Under Secretary of Homeland Security for Intelligence and Analysis, and any other official of the Department of Homeland Security designated by the Secretary of Homeland Security, in sponsoring a security clearance up to the top secret level for each eligible chief election official of a State or the District of Columbia, and additional eligible designees of such election official as appropriate, at the time that such election official assumes such position.

(2) Interim clearances

Consistent with applicable policies and directives, the Director of National Intelligence may issue interim clearances, for a period to be determined by the Director, to a chief election official as described in paragraph (1) and up to one designee of such official under such paragraph.

(c) Information sharing

(1) In general

The Director of National Intelligence shall assist the Under Secretary of Homeland Security for Intelligence and Analysis and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 113(a)(1)(H) of title 6) with sharing any appropriate classified information related to threats to election systems and to the integrity of the election process with chief election officials and such designees who have received a security clearance under subsection (b).

(2) Coordination

The Under Secretary of Homeland Security for Intelligence and Analysis shall coordinate with the Director of National Intelligence and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 113(a)(1)(H) of title 6) to facilitate the sharing of information to the affected Secretaries of State or States.

(Pub. L. 116-92, div. E, title LXV, § 6506, Dec. 20, 2019, 133 Stat. 2206.)

§ 3371c. Notification of significant foreign cyber intrusions and active measures campaigns directed at elections for Federal offices

(a) Definitions

In this section:

(1) Active measures campaign

The term “active measures campaign” means a foreign semi-covert or covert intelligence operation.

(2) Candidate, election, and political party

The terms “candidate”, “election”, and “political party” have the meanings given those terms in section 30101 of title 52.

(3) Congressional leadership

The term “congressional leadership” includes the following:

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

(D) The minority leader of the House of Representatives.

(4) Cyber intrusion

The term “cyber intrusion” means an electronic occurrence that actually or imminently jeopardizes, without lawful authority, electronic election infrastructure, or the integrity, confidentiality, or availability of information within such infrastructure.

(5) Electronic election infrastructure

The term “electronic election infrastructure” means an electronic information system of any of the following that is related to an election for Federal office:

(A) The Federal Government.

(B) A State or local government.

(C) A political party.

(D) The election campaign of a candidate.

(6) Federal office

The term “Federal office” has the meaning given that term in section 30101 of title 52.

(7) High confidence

The term “high confidence”, with respect to a determination, means that the determination is based on high-quality information from multiple sources.

(8) Moderate confidence

The term “moderate confidence”, with respect to a determination, means that a determination is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

(9) Other appropriate congressional committees

The term “other appropriate congressional committees” means—

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

(B) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(b) Determinations of significant foreign cyber intrusions and active measures campaigns

The Director of National Intelligence, the Director of the Federal Bureau of Investigation,

and the Secretary of Homeland Security shall jointly carry out subsection (c) if such Directors and the Secretary jointly determine—

(1) that on or after December 20, 2019, a significant foreign cyber intrusion or active measures campaign intended to influence an upcoming election for any Federal office has occurred or is occurring; and

(2) with moderate or high confidence, that such intrusion or campaign can be attributed to a foreign state or to a foreign nonstate person, group, or other entity.

(c) Briefing

(1) In general

Not later than 14 days after making a determination under subsection (b), the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security shall jointly provide a briefing to the congressional leadership, the congressional intelligence committees and, consistent with the protection of sources and methods, the other appropriate congressional committees. The briefing shall be classified and address, at a minimum, the following:

(A) A description of the significant foreign cyber intrusion or active measures campaign, as the case may be, covered by the determination.

(B) An identification of the foreign state or foreign nonstate person, group, or other entity, to which such intrusion or campaign has been attributed.

(C) The desirability and feasibility of the public release of information about the cyber intrusion or active measures campaign.

(D) Any other information such Directors and the Secretary jointly determine appropriate.

(2) Electronic election infrastructure briefings

With respect to a significant foreign cyber intrusion covered by a determination under subsection (b), the Secretary of Homeland Security, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall offer to the owner or operator of any electronic election infrastructure directly affected by such intrusion, a briefing on such intrusion, including steps that may be taken to mitigate such intrusion. Such briefing may be classified and made available only to individuals with appropriate security clearances.

(3) Protection of sources and methods

This subsection shall be carried out in a manner that is consistent with the protection of sources and methods.

(Pub. L. 116–92, div. E, title LXV, § 6507, Dec. 20, 2019, 133 Stat. 2207.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3371d. Designation of counterintelligence officer to lead election security matters

(a) In general

The Director of National Intelligence shall designate a national counterintelligence officer within the National Counterintelligence and Security Center to lead, manage, and coordinate counterintelligence matters relating to election security.

(b) Additional responsibilities

The person designated under subsection (a) shall also lead, manage, and coordinate counterintelligence matters relating to risks posed by interference from foreign powers (as defined in section 1801 of this title) to the following:

(1) The Federal Government election security supply chain.

(2) Election voting systems and software.

(3) Voter registration databases.

(4) Critical infrastructure related to elections.

(5) Such other Government goods and services as the Director of National Intelligence considers appropriate.

(Pub. L. 116–92, div. E, title LXV, § 6508, Dec. 20, 2019, 133 Stat. 2208.)

§ 3372. Monitoring mineral investments under Belt and Road Initiative of People's Republic of China

(a) Report required

Not later than 1 year after December 27, 2020, the Director of National Intelligence (referred to in this section as the “Director”), in consultation with the Secretary of the Interior, the Secretary of Energy, the Secretary of Commerce, the Secretary of State, the Secretary of Defense, and the United States Trade Representative, shall submit to the appropriate congressional committees a report on investments in minerals under the Belt and Road Initiative of the People's Republic of China that includes an assessment of—

(1) notable past mineral investments;

(2) whether and how such investments have increased the extent of control of minerals by the People's Republic of China;

(3) any efforts by the People's Republic of China to counter or interfere with the goals of the Energy Resource Governance Initiative of the Department of State; and

(4) the strategy of the People's Republic of China with respect to mineral investments.

(b) Monitoring mechanism

In conjunction with each report required by subsection (a), the Director shall submit to the appropriate congressional committees a list of any minerals with respect to which—

(1) the People's Republic of China, directly or through the Belt and Road Initiative—

(A) is increasing its concentration of extraction and processing;

(B) is acquiring significant mining and processing facilities;

(C) is maintaining or increasing export restrictions; or

(D) has achieved substantial control of the supply of minerals used within an industry or related minerals;

(2) there is a significant difference between domestic prices in the People's Republic of China as compared to prices on international markets; or

(3) there is a significant increase or volatility in price as a result of the Belt and Road Initiative of the People's Republic of China.

(c) Critical mineral evaluation

For any mineral included on the list required by subsection (b) that is not already designated as critical by the Secretary of the Interior pursuant to section 1606(c) of title 30, the Director shall—

(1) determine, in consultation with the Secretary of the Interior, the Secretary of Energy, the Secretary of Commerce, the Secretary of State, the Secretary of Defense, and the United States Trade Representative, whether the mineral is strategic and critical to the defense or national security of the United States; and

(2) make a recommendation to the Secretary of the Interior regarding the designation of the mineral under section 1606(c) of title 30.

(d) Annual updates

The Director shall update the report required by subsection (a) and list required by subsection (b) not less frequently than annually.

(e) Form

Each report or list required by this section shall be submitted in unclassified form but may include a classified annex.

(f) Appropriate congressional committees defined

In this section, the term “appropriate congressional committees” means—

(1) the Committee on Energy and Natural Resources, the Committee on Foreign Relations, the Committee on Armed Services, the Committee on Finance, the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the Senate; and

(2) the Committee on Energy and Commerce, the Committee on Foreign Affairs, the Committee on Armed Services, the Committee on Ways and Means, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(Pub. L. 116-260, div. Z, title VII, § 7003, Dec. 27, 2020, 134 Stat. 2577.)

§ 3373. Establishment of All-domain Anomaly Resolution Office

(a) Establishment of Office

(1) In general

Not later than 120 days after December 23, 2022, the Secretary of Defense, in coordination with the Director of National Intelligence, shall establish an office within a component of the Office of the Secretary of Defense, or within a joint organization of the Department of Defense and the Office of the Director of National Intelligence, to carry out the duties of the Unidentified Aerial Phenomena Task Force, as in effect on December 26, 2021, and

such other duties as are required by this section, including those pertaining to unidentified anomalous phenomena.

(2) Designation

The office established under paragraph (1) shall be known as the “All-domain Anomaly Resolution Office” (in this section referred to as the “Office”).

(b) Director and Deputy Director of the Office

(1) Appointment of Director

The head of the Office shall be the Director of the All-domain Anomaly Resolution Office (in this section referred to as the “Director of the Office”), who shall be appointed by the Secretary of Defense in consultation with the Director of National Intelligence.

(2) Appointment of Deputy Director

The Deputy Director of the Office shall be appointed by the Director of National Intelligence in coordination with the Secretary of Defense.

(3) Reporting

(A) In general

The Director of the Office shall report directly to the Deputy Secretary of Defense and the Principal Deputy Director of National Intelligence.

(B) Administrative and operational and security matters

The Director of the Office shall report—

(i) to the Under Secretary of Defense for Intelligence and Security on all administrative matters of the Office; and

(ii) to the Deputy Secretary of Defense and the Principal Deputy Director of National Intelligence on all operational and security matters of the Office.

(c) Duties

The duties of the Office shall include the following:

(1) Developing procedures to synchronize and standardize the collection, reporting, and analysis of incidents, including adverse physiological effects, regarding unidentified anomalous phenomena across the Department of Defense and the intelligence community, in coordination with the Director of National Intelligence, which shall be provided to the congressional defense committees, the congressional intelligence committees, and congressional leadership.

(2) Developing processes and procedures to ensure that such incidents from each component of the Department and each element of the intelligence community are reported and stored in an appropriate manner that allows for the integration of analysis of such information.

(3) Establishing procedures to require the timely and consistent reporting of such incidents.

(4) Evaluating links between unidentified anomalous phenomena and adversarial foreign governments, other foreign governments, or nonstate actors.

(5) Evaluating the threat that such incidents present to the United States.

(6) Coordinating with other departments and agencies of the Federal Government, as appropriate, including the Federal Aviation Administration, the National Aeronautics and Space Administration, the Department of Homeland Security, the National Oceanic and Atmospheric Administration, the National Science Foundation, and the Department of Energy.

(7) As appropriate, and in coordination with the Secretary of State, the Secretary of Defense, and the Director of National Intelligence, consulting with allies and partners of the United States to better assess the nature and extent of unidentified anomalous phenomena.

(8) Preparing reports for Congress, in both classified and unclassified form, including under subsection (j).

(d) Response to and field investigations of unidentified anomalous phenomena

(1) Designation

The Secretary of Defense and the Director of National Intelligence shall jointly designate from within their respective organizations an official, to be under the direction of the Director of the Office, responsible for ensuring the appropriate expertise, authorities, accesses, data, systems, platforms, and capabilities are available for the rapid response to, and support for, the conduct of field investigations of incidents involving unidentified anomalous phenomena.

(2) Ability to respond

The Secretary of Defense and the Director of National Intelligence shall ensure field investigations are supported by personnel with the requisite expertise, equipment, transportation, and other resources necessary to respond rapidly to incidents or patterns of observations involving unidentified anomalous phenomena.

(e) Scientific, technological, and operational analyses of data on unidentified anomalous phenomena

(1) Designation

The Secretary of Defense, in coordination with the Director of National Intelligence, shall designate one or more line organizations that will be primarily responsible for scientific, technical, and operational analysis of data gathered by field investigations conducted pursuant to subsection (d) and data from other sources, including with respect to the testing of materials, medical studies, and development of theoretical models, to better understand and explain unidentified anomalous phenomena.

(2) Authority

The Secretary of Defense and the Director of National Intelligence shall each issue such directives as are necessary to ensure that each line organization designated under paragraph (1) has authority to draw on the special expertise of persons outside the Federal Government with appropriate security clearances.

(f) Data; intelligence collection

(1) Availability of data and reporting on unidentified anomalous phenomena

(A) Availability of data

The Director of National Intelligence, in coordination with the Secretary of Defense, shall ensure that each element of the intelligence community with data relating to unidentified anomalous phenomena makes such data available immediately to the Office.

(B) Reporting

The Director of National Intelligence and the Secretary of Defense shall each, in coordination with one another, ensure that military and civilian personnel of the Department of Defense or an element of the intelligence community, and contractor personnel of the Department or such an element, have access to procedures by which the personnel shall report incidents or information, including adverse physiological effects, involving or associated with unidentified anomalous phenomena directly to the Office.

(2) Intelligence collection and analysis plan

The Director of the Office, acting in coordination with the Secretary of Defense and the Director of National Intelligence, shall supervise the development and execution of an intelligence collection and analysis plan to gain as much knowledge as possible regarding the technical and operational characteristics, origins, and intentions of unidentified anomalous phenomena, including with respect to the development, acquisition, deployment, and operation of technical collection capabilities necessary to detect, identify, and scientifically characterize unidentified anomalous phenomena.

(3) Use of resources and capabilities

In developing the plan under paragraph (2), the Director of the Office shall consider and propose, as appropriate, the use of any resource, capability, asset, or process of the Department and the intelligence community.

(g) Science plan

The Director of the Office, on behalf of the Secretary of Defense and the Director of National Intelligence, shall supervise the development and execution of a science plan to develop and test, as practicable, scientific theories to—

(1) account for characteristics and performance of unidentified anomalous phenomena that exceed the known state of the art in science or technology, including in the areas of propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, and power generation; and

(2) provide the foundation for potential future investments to replicate or otherwise better understand any such advanced characteristics and performance.

(h) Assignment of priority

The Director of National Intelligence, in consultation with and with the recommendation of

the Secretary of Defense, shall assign an appropriate level of priority within the National Intelligence Priorities Framework to the requirement to understand, characterize, and respond to unidentified anomalous phenomena.

(i) Detailees from elements of the intelligence community

The heads of the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the Department of Energy, the National Geospatial-Intelligence Agency, the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard, the Department of Homeland Security, and such other elements of the intelligence community as the Director of the Office considers appropriate may provide to the Office a detailee of the element to be physically located at the Office.

(j) Historical record report

(1) Report required

(A) In general

Not later than 540 days after December 23, 2022, the Director of the Office shall submit to the congressional defense committees, the congressional intelligence committees, and congressional leadership a written report detailing the historical record of the United States Government relating to unidentified anomalous phenomena, including—

- (i) the records and documents of the intelligence community;
- (ii) oral history interviews;
- (iii) open source analysis;
- (iv) interviews of current and former Government officials;
- (v) classified and unclassified national archives including any records any third party obtained pursuant to section 552 of title 5; and
- (vi) such other relevant historical sources as the Director of the Office considers appropriate.

(B) Other requirements

The report submitted under subparagraph (A) shall—

- (i) focus on the period beginning on January 1, 1945, and ending on the date on which the Director of the Office completes activities under this subsection; and
- (ii) include a compilation and itemization of the key historical record of the involvement of the intelligence community with unidentified anomalous phenomena, including—
 - (I) any program or activity that was protected by restricted access that has not been explicitly and clearly reported to Congress;
 - (II) successful or unsuccessful efforts to identify and track unidentified anomalous phenomena; and
 - (III) any efforts to obfuscate, manipulate public opinion, hide, or otherwise provide incorrect unclassified or classified information about unidentified anomalous phenomena or related activities.

(2) Access to records of the National Archives and Records Administration

The Archivist of the United States shall make available to the Office such information maintained by the National Archives and Records Administration, including classified information, as the Director of the Office considers necessary to carry out paragraph (1).

(k) Annual reports

(1) Reports from All-domain Anomaly Resolution Office

(A) Requirement

Not later than 180 days after December 23, 2022, and annually thereafter for four years, the Director of the Office shall submit to the appropriate congressional committees a report on unidentified anomalous phenomena.

(B) Elements

Each report submitted under subparagraph (A) shall include, with respect to the year covered by the report, the following information:

- (i) All reported unidentified anomalous phenomena-related events that occurred during the one-year period.
- (ii) All reported unidentified anomalous phenomena-related events that occurred during a period other than that one-year period but were not included in an earlier report.
- (iii) An analysis of data and intelligence received through each reported unidentified anomalous phenomena-related event.
- (iv) An analysis of data relating to unidentified anomalous phenomena collected through—
 - (I) geospatial intelligence;
 - (II) signals intelligence;
 - (III) human intelligence; and
 - (IV) measurement and signature intelligence.
- (v) The number of reported incidents of unidentified anomalous phenomena over restricted airspace of the United States during the one-year period.
- (vi) An analysis of such incidents identified under clause (v).
- (vii) Identification of potential aerospace or other threats posed by unidentified anomalous phenomena to the national security of the United States.
- (viii) An assessment of any activity regarding unidentified anomalous phenomena that can be attributed to one or more adversarial foreign governments.
- (ix) Identification of any incidents or patterns regarding unidentified anomalous phenomena that indicate a potential adversarial foreign government may have achieved a breakthrough aerospace capability.
- (x) An update on the coordination by the United States with allies and partners on efforts to track, understand, and address unidentified anomalous phenomena.
- (xi) An update on any efforts underway on the ability to capture or exploit discovered unidentified anomalous phenomena.

(xii) An assessment of any health-related effects for individuals that have encountered unidentified anomalous phenomena.

(xiii) The number of reported incidents, and descriptions thereof, of unidentified anomalous phenomena associated with military nuclear assets, including strategic nuclear weapons and nuclear-powered ships and submarines.

(xiv) In consultation with the Administrator for Nuclear Security, the number of reported incidents, and descriptions thereof, of unidentified anomalous phenomena associated with facilities or assets associated with the production, transportation, or storage of nuclear weapons or components thereof.

(xv) In consultation with the Chairman of the Nuclear Regulatory Commission, the number of reported incidents, and descriptions thereof, of unidentified anomalous phenomena or drones of unknown origin associated with nuclear power generating stations, nuclear fuel storage sites, or other sites or facilities regulated by the Nuclear Regulatory Commission.

(xvi) The names of the line organizations that have been designated to perform the specific functions under subsections (d) and (e), and the specific functions for which each such line organization has been assigned primary responsibility.

(xvii) A summary of the reports received using the mechanism for authorized reporting established under section 3373b of this title.

(2) Form

Each report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(I) Semiannual briefings

(1) Requirement

Not later than December 31, 2022, and not less frequently than semiannually thereafter until December 31, 2026, the Director of the Office shall provide to the appropriate congressional committees classified briefings on unidentified anomalous phenomena.

(2) First briefing

The first briefing provided under paragraph (1) shall include all incidents involving unidentified anomalous phenomena that were reported to the Unidentified Aerial Phenomena Task Force or to the Office established under subsection (a) after June 24, 2021, regardless of the date of occurrence of the incident.

(3) Subsequent briefings

Each briefing provided subsequent to the first briefing described in paragraph (2) shall include, at a minimum, all events relating to unidentified anomalous phenomena that occurred during the previous 180 days, and events relating to unidentified anomalous phenomena that were not included in an earlier briefing.

(4) Instances in which data was not shared

For each briefing period, the Director of the Office shall jointly provide to the chairman or

chair and the ranking member or vice chairman of the congressional committees specified in subparagraphs (A) and (D) of subsection (n)(1) an enumeration of any instances in which data relating to unidentified anomalous phenomena was not provided to the Office because of classification restrictions on that data or for any other reason.

(m) Task Force termination

Not later than the date on which the Secretary of Defense establishes the Office under subsection (a), the Secretary shall terminate the Unidentified Aerial Phenomena Task Force.

(n) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means the following:

(A) The Committees on Armed Services of the Senate and the House of Representatives.

(B) The Committees on Appropriations of the Senate and the House of Representatives.

(C) The Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(D) The Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(E) The Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

(F) The Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(2) Congressional defense committees

The term “congressional defense committees” has the meaning given such term in section 101(a) of title 10.

(3) Congressional intelligence committees

The term “congressional intelligence committees” has the meaning given such term in section 3003 of this title.

(4) Congressional leadership

The term “congressional leadership” means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(5) Intelligence community

The term “intelligence community” has the meaning given such term in section 3003 of this title.

(6) Line organization

The term “line organization” means, with respect to a department or agency of the Federal Government, an organization that executes programs and activities to directly advance the core functions and missions of the

department or agency to which the organization is subordinate, but, with respect to the Department of Defense, does not include a component of the Office of the Secretary of Defense.

(7) Transmedium objects or devices

The term “transmedium objects or devices” means objects or devices that are—

- (A) observed to transition between space and the atmosphere, or between the atmosphere and bodies of water; and
- (B) not immediately identifiable.

(8) Unidentified anomalous phenomena

The term “unidentified anomalous phenomena” means—

- (A) airborne objects that are not immediately identifiable;
- (B) transmedium objects or devices; and
- (C) submerged objects or devices that are not immediately identifiable and that display behavior or performance characteristics suggesting that the objects or devices may be related to the objects described in subparagraph (A).

(Pub. L. 117–81, div. A, title XVI, § 1683, Dec. 27, 2021, 135 Stat. 2118; Pub. L. 117–263, div. A, title XVI, § 1673(c), div. F, title LXVIII, § 6802(a), Dec. 23, 2022, 136 Stat. 2961, 3586; Pub. L. 118–31, div. G, title III, § 7341, Dec. 22, 2023, 137 Stat. 1062.)

Editorial Notes

AMENDMENTS

2023—Subsec. (k)(1). Pub. L. 118–31, § 7341(1), substituted “All-domain Anomaly Resolution Office” for “Director of National Intelligence and Secretary of Defense” in heading.

Subsec. (k)(1)(A). Pub. L. 118–31, § 7341(2), substituted “Director of the Office shall” for “Director of National Intelligence and the Secretary of Defense shall jointly”.

2022—Pub. L. 117–263, § 6802(a), amended section generally. Prior to amendment, section established an office, organizational structure, and authorities to address unidentified anomalous phenomena.

Pub. L. 117–263, § 1673(c)(1), substituted “anomalous” for “aerial” wherever appearing.

Subsec. (h)(1). Pub. L. 117–263, § 1673(c)(2)(A), inserted “and the congressional leadership” after “appropriate congressional committees”.

Subsec. (h)(2)(Q). Pub. L. 117–263, § 1673(c)(2)(B), added subpar. (Q).

Subsec. (l)(2) to (6). Pub. L. 117–263, § 1673(c)(3), added par. (2) and redesignated former pars. (2) to (5) as (3) to (6), respectively.

Statutory Notes and Related Subsidiaries

LIAISON WITH COUNTER UNMANNED AERIAL SYSTEMS TASK FORCE

Pub. L. 118–159, div. A, title X, § 1089, Dec. 23, 2024, 138 Stat. 2081, provided that:

“(a) **LIAISON REQUIRED.**—The Director of the All-Domain Anomaly Resolution Office of the Department of Defense shall designate one or more employees of the Office to act as a liaison with the Counter Unmanned Aerial Systems Task Force established under section 925 [of Pub. L. 118–159, 10 U.S.C. 130i note] to improve coordination of efforts and support enabling capabilities of mutual benefit.

“(b) **RESPONSIBILITIES.**—An individual designated as a liaison under subsection (a) shall have the following responsibilities:

“(1) Conducting information sharing between the Office and the Task Force on identified or suspected Unmanned Aerial Systems events, including incident reporting, incident responses, and data on technical characterization of the known or suspected threats.

“(2) Coordinating the development of technical capabilities for sensing and response to threats.

“(3) Developing coordinated tactics, techniques, and procedures for incident response.”

LIMITATION REGARDING INDEPENDENT RESEARCH AND DEVELOPMENT

Pub. L. 118–31, div. A, title XVI, § 1687(b), (c), Dec. 22, 2023, 137 Stat. 621, provided that:

“(b) **LIMITATION REGARDING INDEPENDENT RESEARCH AND DEVELOPMENT.**—Consistent with Department of Defense Instruction Number 3204.01 (dated August 20, 2014, incorporating change 2, dated July 9, 2020; relating to Department policy for oversight of independent research and development), independent research and development funding relating to unidentified anomalous phenomena shall not be allowable as indirect expenses for purposes of contracts covered by such instruction, unless such material and information is made available to the appropriate congressional committees and congressional leadership.

“(c) **DEFINITIONS.**—In this section:

“(1) The term ‘appropriate congressional committees’ means—

“(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives]; and

“(B) the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

“(2) The term ‘congressional leadership’ means—

“(A) the majority leader of the Senate;

“(B) the minority leader of the Senate;

“(C) the Speaker of the House of Representatives; and

“(D) the minority leader of the House of Representatives.

“(3) The term ‘unidentified anomalous phenomena’ has the meaning given such term in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)), as amended by section 6802(a) of the Intelligence Authorization Act for Fiscal Year 2023 ([div. F of] Public Law 117–263).”

COMPTROLLER GENERAL OF THE UNITED STATES AUDITS AND BRIEFINGS ON UNIDENTIFIED ANOMALOUS PHENOMENA HISTORICAL RECORD REPORT

Pub. L. 117–263, div. F, title LXVIII, § 6803, Dec. 23, 2022, 136 Stat. 3594, as amended by Pub. L. 118–159, div. F, title LXVIII, § 6802, Dec. 23, 2024, 138 Stat. 2516, provided that:

“(a) **DEFINITIONS.**—In this section, the terms ‘congressional leadership’ and ‘Office’ have the meanings given such terms in section 1683 of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373), as amended by section 6802.

“(b) **AUDIT.**—

“(1) **IN GENERAL.**—Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2022], the Comptroller General of the United States shall identify appropriately cleared personnel of the Government Accountability Office to audit the historical record report process described in section 1683 of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373), as amended by section 6802, including personnel to conduct work on-site as appropriate.

“(2) **PROVISION OF INFORMATION.**—On a quarterly basis until the date that is 90 days after the delivery of the final volume of the Historical Record Report, and as appropriate and consistent with Government Auditing Standards, the Comptroller General of the United States shall provide the Office with information on the findings of any audits conducted by the personnel identified under paragraph (1).

“(c) VERBAL BRIEFINGS.—Not later than 180 days after the date of the enactment of this Act, and semiannually thereafter until the date that is 180 days after the delivery of the final volume of the Historical Record Report, the Comptroller General of the United States shall verbally brief the congressional intelligence committees, the congressional defense committees, and congressional leadership on the progress of the Office with respect to the historical record report described in section 1683 of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373), as amended by section 6802, and compliance with legislative requirements.

“(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to restrict access of a committee of Congress under section 719(f) of title 31, United States Code, to an audit under subsection (b).”

[For definition of “congressional intelligence committees” as used in section 6803 of Pub. L. 117–263, set out above, see section 6002 of Pub. L. 117–263, set out as a note under section 3003 of this title.]

§ 3373a. Support for and oversight of Unidentified Aerial Phenomena Task Force

(a) Availability of data on unidentified aerial phenomena

The Director of National Intelligence and the Secretary of Defense shall jointly require that each element of the intelligence community and component of the Department of Defense with data relating to unidentified aerial phenomena makes¹ such data available immediately to the Unidentified Aerial Phenomena Task Force, or successor entity, and to the National Air and Space Intelligence Center.

(b) Quarterly reports

(1) In general

Not later than 90 days after March 15, 2022, and not less frequently than quarterly thereafter, the Unidentified Aerial Phenomena Task Force, or successor entity, consistent with the protection of intelligence sources and methods, shall submit to the appropriate congressional committees a report on the findings of the Unidentified Aerial Phenomena Task Force, or successor entity.

(2) Contents

Each report submitted under paragraph (1) shall include, at a minimum, the following:

(A) All reported unidentified aerial phenomena-related events that occurred during the period covered by the report.

(B) All reported unidentified aerial phenomena-related events that occurred during a period other than the period covered by the report but were not included in an earlier report.

(3) Form

Each report submitted under paragraph (1) shall be submitted in classified form.

(c) Definitions

In this section:

(1) Appropriate congressional committees

The term “appropriate congressional committees” means the following:

(A) The congressional intelligence committees.

(B) The Committees on Armed Services of the House of Representatives and the Senate.

(2) Unidentified Aerial Phenomena Task Force

The term “Unidentified Aerial Phenomena Task Force” means the task force established by the Department of Defense on August 4, 2020, to be led by the Department of the Navy, under the Office of the Under Secretary of Defense for Intelligence and Security.

(Pub. L. 117–103, div. X, title IV, §413, Mar. 15, 2022, 136 Stat. 977.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “congressional intelligence committees” and “intelligence community” as used in this section, see section 2 of div. X of Pub. L. 117–103, set out as a note under section 3003 of this title.

§ 3373b. Unidentified anomalous phenomena reporting procedures

(a) Mechanism for authorized reporting

(1) Establishment

The Secretary of Defense, acting through the head of the Office and in consultation with the Director of National Intelligence, shall establish a secure mechanism for authorized reporting of—

(A) any event relating to unidentified anomalous phenomena; and

(B) any activity or program by a department or agency of the Federal Government or a contractor of such a department or agency relating to unidentified anomalous phenomena, including with respect to material retrieval, material analysis, reverse engineering, research and development, detection and tracking, developmental or operational testing, and security protections and enforcement.

(2) Protection of systems, programs, and activity

The Secretary shall ensure that the mechanism for authorized reporting established under paragraph (1) prevents the unauthorized public reporting or compromise of classified military and intelligence systems, programs, and related activity, including all categories and levels of special access and compartmented access programs.

(3) Administration

The Secretary shall ensure that the mechanism for authorized reporting established under paragraph (1) is administered by designated and appropriately cleared employees of the Department of Defense or elements of the intelligence community or contractors of the Department or such elements assigned to the Office.

(4) Sharing of information

(A) Prompt sharing within Office

The Secretary shall ensure that the mechanism for authorized reporting established under paragraph (1) provides for the sharing of an authorized disclosure to personnel and

¹ So in original. Probably should be “make”.

supporting analysts and scientists of the Office (regardless of the classification of information contained in the disclosure or any nondisclosure agreements), unless the employees or contractors administering the mechanism under paragraph (3) conclude that the preponderance of information available regarding the disclosure indicates that the observed object and associated events and activities likely relate to a special access program or compartmented access program that, as of the date of the disclosure, has been explicitly and clearly reported to the congressional defense committees or the congressional intelligence committees, and is documented as meeting those criteria.

(B) Congressional notification

Not later than 72 hours after determining that an authorized disclosure relates to a restricted access activity, a special access program, or a compartmented access program that has not been explicitly and clearly reported to the congressional defense committees or the congressional intelligence committees, the Secretary shall report such disclosure to such committees and the congressional leadership.

(5) Initial report and publication

Not later than 180 days after December 23, 2022, the Secretary, acting through the head of the Office and in consultation with the Director of National Intelligence, shall—

(A) submit to the congressional defense committees, the congressional intelligence committees, and the congressional leadership a report detailing the mechanism for authorized reporting established under paragraph (1); and

(B) issue clear public guidance for how to securely access the mechanism for authorized reporting.

(b) Protection for individuals making authorized disclosures

(1) Authorized disclosures

An authorized disclosure—

(A) shall not be subject to a nondisclosure agreement entered into by the individual who makes the disclosure;

(B) shall be deemed to comply with any regulation or order issued under the authority of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information) or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); and

(C) is not a violation of section 798 of title 18 or other provision of law relating to the disclosure of information.

(2) Prohibition on reprisals

(A) Protection

An employee of a department or agency of the Federal Government, or of a contractor, subcontractor, grantee, subgrantee, or personal services contractor of such a department or agency, who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a

personnel action, including the revocation or suspension of security clearances, or termination of employment, with respect to any individual as a reprisal for any authorized disclosure.

(B) Procedures

The Secretary of Defense and the Director of National Intelligence shall establish procedures for the enforcement of subparagraph (A) consistent with, as appropriate, section 1034 of title 10, section 3234 of title 50, or other similar provisions of law regarding prohibited personnel actions.

(3) Nondisclosure agreements

(A) Identification

The Secretary of Defense, the Director of National Intelligence, the Secretary of Homeland Security, the heads of such other departments and agencies of the Federal Government that have supported investigations of the types of events covered by subparagraph (A) of subsection (a)(1) and activities and programs described in subparagraph (B) of such subsection, and contractors of the Federal Government that have supported or are supporting such activities and programs, shall conduct comprehensive searches of all records relating to nondisclosure orders relating to the types of events described in subsection (a) and provide copies of such orders, agreements, or obligations to the Office.

(B) Submission to Congress

The head of the Office shall—

(i) make the records compiled under subparagraph (A) accessible to the congressional defense committees, the congressional intelligence committees, and the congressional leadership; and

(ii) not later than September 30, 2023, and at least once each fiscal year thereafter through fiscal year 2026, provide to such committees and congressional leadership briefings and reports on such records.

(c) Omitted

(d) Definitions

In this section:

(1) The term “authorized disclosure” means a report of any information through, and in compliance with, the mechanism for authorized reporting established pursuant to subsection (a)(1).

(2) The term “congressional intelligence committees” has the meaning given such term in section 3003 of this title.

(3) The term “congressional leadership” means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(4) The term “intelligence community” has the meaning given such term in section 3003 of this title.

(5) The term “nondisclosure agreement” means any written or oral nondisclosure

agreement, order, or other instrumentality or means entered into by an individual that could be interpreted as a legal constraint on the individual making an authorized disclosure.

(6) The term “Office” means the All-domain Anomaly Resolution Office established pursuant to section 3373(a) of this title.

(7) The term “personnel action” has the meaning given such term in section 3234(a) of this title.

(8) The term “unidentified anomalous phenomena” has the meaning given such term in section 3373(n) of this title.

(Pub. L. 117-263, div. A, title XVI, § 1673, Dec. 23, 2022, 136 Stat. 2959.)

Editorial Notes

REFERENCES IN TEXT

Executive Order 13526, referred to in subsec. (b)(1)(B), is Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, 1013, which is set out as a note under section 3161 of this title.

The Atomic Energy Act of 1954, referred to in subsec. (b)(1)(B), is act Aug. 1, 1946, ch. 724, as added by act Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 919. Chapter 18 of the Act is classified generally to subchapter XVII (§ 2271 et seq.) of chapter 23 of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 42 and Tables.

CODIFICATION

Section is comprised of section 1673 of Pub. L. 117-263. Subsec. (c) of section 1673 of Pub. L. 117-263 amended section 3373 of this title.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional defense committees” as the Committees on Armed Services and Appropriations of the Senate and the House of Representatives, see section 101 of Title 10, Armed Forces, as made applicable by section 3 of of Pub. L. 117-263, which is listed in a table under section 101 of Title 10.

SUBCHAPTER V—MANAGEMENT OF COUNTERINTELLIGENCE ACTIVITIES

§ 3381. Coordination of counterintelligence activities

(a) Establishment of Counterintelligence Policy Board

There is established within the executive branch of Government a National Counterintelligence Policy Board (in this section referred to as the “Board”). The Board shall report to the President through the National Security Council.

(b) Chairperson

The Director of the National Counterintelligence and Security Center appointed under section 902 of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3382) shall serve as the chairperson of the Board.

(c) Membership

The membership of the National Counterintelligence Policy Board shall consist of the following:

(1) The Director of the National Counterintelligence and Security Center.

(2) Senior personnel of departments and elements of the United States Government, appointed by the head of the department or element concerned, as follows:

(A) The Department of Justice, including the Federal Bureau of Investigation.

(B) The Department of Defense, including the Joint Chiefs of Staff.

(C) The Department of State.

(D) The Department of Energy.

(E) The Central Intelligence Agency.

(F) Any other department, agency, or element of the United States Government specified by the President.

(d) Functions and discharge of functions

(1) The Board shall—

(A) serve as the principal mechanism for—

(i) developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities; and

(ii) upon the direction of the President, resolving conflicts that arise between elements of the Government conducting such activities; and

(B) act as an interagency working group to—

(i) ensure the discussion and review of matters relating to the implementation of the Counterintelligence Enhancement Act of 2002; and

(ii) provide advice to the Director of the National Counterintelligence and Security Center on priorities in the implementation of the National Counterintelligence Strategy produced pursuant to section 904(e)(2) of that Act (50 U.S.C. 3383(e)(2)).

(2) The Board may, for purposes of carrying out its functions under this section, establish such interagency boards and working groups as the Board considers appropriate.

(e) Coordination of counterintelligence matters with Federal Bureau of Investigation

(1) Except as provided in paragraph (5), the head of each department or agency within the executive branch shall ensure that—

(A) the Federal Bureau of Investigation is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power;

(B) following a report made pursuant to subparagraph (A), the Federal Bureau of Investigation is consulted with respect to all subsequent actions which may be undertaken by the department or agency concerned to determine the source of such loss or compromise; and

(C) where, after appropriate consultation with the department or agency concerned, the Federal Bureau of Investigation undertakes investigative activities to determine the source of the loss or compromise, the Federal Bureau of Investigation is given complete and timely access to the employees and records of the department or agency concerned for purposes of such investigative activities.

(2) Except as provided in paragraph (5), the Director of the Federal Bureau of Investigation

shall ensure that espionage information obtained by the Federal Bureau of Investigation pertaining to the personnel, operations, or information of departments or agencies of the executive branch, is provided through appropriate channels in a timely manner to the department or agency concerned, and that such departments or agencies are consulted in a timely manner with respect to espionage investigations undertaken by the Federal Bureau of Investigation which involve the personnel, operations, or information of such department or agency.

(3)(A) The Director of the Federal Bureau of Investigation shall submit to the head of the department or agency concerned a written assessment of the potential impact of the actions of the department or agency on a counterintelligence investigation.

(B) The head of the department or agency concerned shall—

(i) use an assessment under subparagraph (A) as an aid in determining whether, and under what circumstances, the subject of an investigation under paragraph (1) should be left in place for investigative purposes; and

(ii) notify in writing the Director of the Federal Bureau of Investigation of such determination.

(C) The Director of the Federal Bureau of Investigation and the head of the department or agency concerned shall continue to consult, as appropriate, to review the status of an investigation covered by this paragraph, and to reassess, as appropriate, a determination of the head of the department or agency concerned to leave a subject in place for investigative purposes.

(4)(A) The Federal Bureau of Investigation shall notify appropriate officials within the executive branch, including the head of the department or agency concerned, of the commencement of a full field espionage investigation with respect to an employee within the executive branch.

(B) A department or agency may not conduct a polygraph examination, interrogate, or otherwise take any action that is likely to alert an employee covered by a notice under subparagraph (A) of an investigation described in that subparagraph without prior coordination and consultation with the Federal Bureau of Investigation.

(5) Where essential to meet extraordinary circumstances affecting vital national security interests of the United States, the President may on a case-by-case basis waive the requirements of paragraph (1), (2), or (3), as they apply to the head of a particular department or agency, or the Director of the Federal Bureau of Investigation. Such waiver shall be in writing and shall fully state the justification for such waiver. Within thirty days, the President shall notify the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives that such waiver has been issued, and at that time or as soon as national security considerations permit, provide these committees with a complete explanation of the circumstances which necessitated such waiver.

(6) Nothing in this section may be construed to alter the existing jurisdictional arrangements

between the Federal Bureau of Investigation and the Department of Defense with respect to investigations of persons subject to the Uniform Code of Military Justice, nor to impose additional reporting requirements upon the Department of Defense with respect to such investigations beyond those required by existing law and executive branch policy.

(7) As used in this section, the terms “foreign power” and “agent of a foreign power” have the same meanings as set forth in subsections (a) and (b) of section 1801, respectively, of this title.

(Pub. L. 103-359, title VIII, § 811, Oct. 14, 1994, 108 Stat. 3455; Pub. L. 106-120, title VI, § 602, Dec. 3, 1999, 113 Stat. 1620; Pub. L. 106-567, title VI, § 605, Dec. 27, 2000, 114 Stat. 2853; Pub. L. 107-306, title VIII, § 811(b)(5)(B), title IX, § 903, Nov. 27, 2002, 116 Stat. 2424, 2433; Pub. L. 108-177, title III, § 361(g), Dec. 13, 2003, 117 Stat. 2625; Pub. L. 108-458, title I, § 1071(g)(1), Dec. 17, 2004, 118 Stat. 3691; Pub. L. 115-31, div. N, title IV, § 401(f), May 5, 2017, 131 Stat. 819; Pub. L. 118-31, div. G, title III, § 7305(b)(2), title IX, § 7901(j), Dec. 22, 2023, 137 Stat. 1026, 1107.)

Editorial Notes

REFERENCES IN TEXT

The Counterintelligence Enhancement Act of 2002, referred to in subsec. (d)(1)(B), is title IX of Pub. L. 107-306, Nov. 27, 2002, 116 Stat. 2432. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was formerly classified to section 402a of this title prior to editorial reclassification and renumbering as this section. Some section numbers of this title referenced in amendment notes below reflect the classification of such sections prior to their editorial reclassification.

AMENDMENTS

2023—Subsec. (d)(1)(B)(ii). Pub. L. 118-31, § 7305(b)(2), substituted “section 904(e)(2) of that Act (50 U.S.C. 3383(e)(2))” for “section 904(d)(2) of that Act (50 U.S.C. 3383(d)(2))”.

Subsec. (e)(7). Pub. L. 118-31, § 7901(j), substituted “subsections (a) and (b) of section 1801” for “sections 1801(a) and (b)”.

2017—Subsec. (b). Pub. L. 115-31, § 401(f)(1), substituted “Director of the National Counterintelligence and Security Center appointed under section 902 of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3382)” for “National Counterintelligence Executive under section 902 of the Counterintelligence Enhancement Act of 2002”.

Subsec. (c)(1). Pub. L. 115-31, § 401(f)(2), substituted “Director of the National Counterintelligence and Security Center.” for “National Counterintelligence Executive.”

Subsec. (d)(1)(B)(ii). Pub. L. 115-31, § 401(f)(3), substituted “Director of the National Counterintelligence and Security Center” for “National Counterintelligence Executive” and “pursuant to section 904(d)(2) of that Act (50 U.S.C. 3383(d)(2))” for “by the Office of the National Counterintelligence Executive under section 904(e)(2) of that Act”.

2004—Subsec. (c)(6)(C). Pub. L. 108-458, which directed amendment of subsec. (c)(6)(C) by substituting “Director of National Intelligence” for “Director of Central Intelligence”, could not be executed because of the amendments by Pub. L. 107-306, § 903(a)(2), and Pub. L. 108-177. See 2002 and 2003 Amendment notes below.

2003—Subsec. (e). Pub. L. 108-177, which directed the amendment of subsec. (c) by redesignating pars. (7) and

(8) as (6) and (7), respectively, and striking out former par. (6), was executed by making the amendment to subsec. (e) to reflect the probable intent of Congress and the redesignation of subsec. (c) as (e) by Pub. L. 107-306, §903(a)(2), see below. Prior to amendment, par. (6) read as follows:

“(6)(A) Not later each year than the date provided in section 415b of this title, the Director of the Federal Bureau of Investigation shall submit to the congressional intelligence committees (as defined in section 401a of this title) a report with respect to compliance with paragraphs (1) and (2) during the previous calendar year.

“(B) Not later than February 1 each year, the Director shall, in accordance with applicable security procedures, submit to the Committees on the Judiciary of the Senate and House of Representatives a report with respect to compliance with paragraphs (1) and (2) during the previous calendar year.

“(C) The Director of the Federal Bureau of Investigation shall submit each report under this paragraph in consultation with the Director of Central Intelligence and the Secretary of Defense.”

2002—Subsec. (b). Pub. L. 107-306, §903(a)(1), (3), added subsec. (b) and struck out heading and text of former subsec. (b). Text read as follows: “The Board shall serve as the principal mechanism for—

“(1) developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities; and

“(2) resolving conflicts, as directed by the President, which may arise between elements of the Government which carry out such activities.”

Subsec. (c). Pub. L. 107-306, §903(b), added subsec. (c). Former subsec. (c) redesignated (e).

Subsec. (c)(6). Pub. L. 107-306, §811(b)(5)(B), amended par. (6) generally. Prior to amendment, par. (6) read as follows: “The Director of the Federal Bureau of Investigation shall, in consultation with the Director of Central Intelligence and the Secretary of Defense, report annually, beginning on February 1, 1995, and continuing each year thereafter, to the Select Committee on Intelligence of the Senate and to the Permanent Select Committee on Intelligence of the House of Representatives and, in accordance with applicable security procedures, the Committees on the Judiciary of the House of Representatives and the Senate with respect to compliance with paragraphs (1) and (2) during the previous calendar year.”

Subsec. (d). Pub. L. 107-306, §903(c), added subsec. (d).

Subsec. (e). Pub. L. 107-306, §903(a)(2), redesignated subsec. (c) as (e).

2000—Subsec. (c)(1). Pub. L. 106-567, §605(a)(1), substituted “paragraph (5)” for “paragraph (3)”.

Subsec. (c)(2). Pub. L. 106-567, §605(a)(1), (b), substituted “paragraph (5)” for “paragraph (3)” and inserted “in a timely manner” after “through appropriate channels” and “are consulted”.

Subsec. (c)(3). Pub. L. 106-567, §605(a)(3), added par. (3). Former par. (3) redesignated (5).

Subsec. (c)(4). Pub. L. 106-567, §605(a), (c), added par. (4). Former par. (4) redesignated (6).

Subsec. (c)(5). Pub. L. 106-567, §605(a)(2), (4), redesignated par. (3) as (5) and substituted “paragraph (1), (2), or (3)” for “paragraph (1) or (2)”. Former par. (5) redesignated (7).

Subsec. (c)(6) to (8). Pub. L. 106-567, §605(a)(2), redesignated pars. (4) to (6) as (6) to (8), respectively.

1999—Subsec. (c)(2). Pub. L. 106-120 struck out “after a report has been provided pursuant to paragraph (1)(A)” before period at end.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108-458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108-458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

EFFECTIVE DATE OF 2003 AMENDMENT

Amendment by Pub. L. 108-177 effective Dec. 31, 2003, see section 361(n) of Pub. L. 108-177, set out as a note under section 1611 of Title 10, Armed Forces.

ANNUAL REPORTS ON INTELLIGENCE ACTIVITIES OF THE PEOPLE'S REPUBLIC OF CHINA

Pub. L. 105-107, title III, §308, Nov. 20, 1997, 111 Stat. 2253, as amended by Pub. L. 107-306, title VIII, §811(b)(5)(D), Nov. 27, 2002, 116 Stat. 2424, related to annual reports to Congress by the Director of Central Intelligence and the Director of the Federal Bureau of Investigation on intelligence activities of the People's Republic of China directed against or affecting the interests of the United States, prior to repeal by Pub. L. 108-177, title III, §361(f), Dec. 13, 2003, 117 Stat. 2625.

§ 3382. Director of the National Counterintelligence and Security Center

(a) Establishment

There shall be a Director of the National Counterintelligence and Security Center (referred to in this section as the “Director”), who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) Mission

The mission of the Director shall be to serve as the head of national counterintelligence for the United States Government.

(c) Duties

Subject to the direction and control of the Director of National Intelligence, the duties of the Director are as follows:

(1) To carry out the mission referred to in subsection (b).

(2) To act as chairperson of the National Counterintelligence Policy Board established under section 3381 of this title.

(3) To act as head of the National Counterintelligence and Security Center established under section 3383 of this title.

(4) To participate as an observer on such boards, committees, and entities of the executive branch as the Director of National Intelligence considers appropriate for the discharge of the mission and functions of the Director and the National Counterintelligence and Security Center under section 3383 of this title.

(Pub. L. 107-306, title IX, §902, Nov. 27, 2002, 116 Stat. 2432; Pub. L. 108-458, title I, §1072(d)(1)(B), Dec. 17, 2004, 118 Stat. 3693; Pub. L. 114-113, div. M, title IV, §401(a), Dec. 18, 2015, 129 Stat. 2920; Pub. L. 115-31, div. N, title IV, §401(a)(1), (3), May 5, 2017, 131 Stat. 816, 817.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 402b of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2017—Pub. L. 115-31, §401(a)(1), amended section generally. Prior to amendment, section related to the National Counterintelligence Executive.

Subsec. (a). Pub. L. 115-31, § 401(a)(3), provided that the amendment made by Pub. L. 114-113, § 401(a), was deemed to not have taken effect. See 2015 Amendment and Effective Date of 2015 Amendment notes below.

2015—Subsec. (a). Pub. L. 114-113, which directed that subsec. (a) be amended to read as follows:

“(a) ESTABLISHMENT.—There shall be a National Counterintelligence Executive who shall be appointed by the President, by and with the advice and consent of the Senate.”,

was deemed to not have taken effect by Pub. L. 115-31, § 401(a)(3). See 2017 Amendment note above.

2004—Subsec. (a)(1). Pub. L. 108-458, § 1072(d)(1)(B)(i), substituted “Director of National Intelligence” for “President”.

Subsec. (a)(2). Pub. L. 108-458, § 1072(d)(1)(B), substituted “Director of National Intelligence” for “President” and “Director of the Central Intelligence Agency” for “Director of Central Intelligence”.

Subsec. (c). Pub. L. 108-458, § 1072(d)(1)(B)(i), substituted “Director of National Intelligence” for “President” in two places.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2015 AMENDMENT

Pub. L. 115-31, div. N, title IV, § 401(a)(3), May 5, 2017, 131 Stat. 817, provided that: “The amendment made by subsection (a) of section 401 of the Intelligence Authorization Act for Fiscal Year 2016 (division M of Public Law 114-113) [amending this section] shall not take effect, or, if the date of the enactment of this Act [May 5, 2017] is on or after the effective date specified in subsection (b) of such section [Dec. 18, 2016, see note below], such amendment shall be deemed to not have taken effect.”

Pub. L. 114-113, div. M, title IV, § 401(b), Dec. 18, 2015, 129 Stat. 2921, provided that: “The amendment made by subsection (a) [amending this section] shall take effect on the date that is one year after the date of the enactment of this Act [Dec. 18, 2015].”

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108-458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108-458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

PURPOSE

Pub. L. 107-306, title IX, § 901(b), Nov. 27, 2002, 116 Stat. 2432, provided that: “The purpose of this title [see Tables for classification] is to facilitate the enhancement of the counterintelligence activities of the United States Government by—

“(1) enabling the counterintelligence community of the United States Government to fulfill better its mission of identifying, assessing, prioritizing, and countering the intelligence threats to the United States;

“(2) ensuring that the counterintelligence community of the United States Government acts in an efficient and effective manner; and

“(3) providing for the integration of all the counterintelligence activities of the United States Government.”

§ 3383. National Counterintelligence and Security Center

(a) Establishment

There shall be a National Counterintelligence and Security Center.

(b) Head of Center

The Director of the National Counterintelligence and Security Center shall be the head of the National Counterintelligence and Security Center.

(c) Location of Center

The National Counterintelligence and Security Center shall be located in the Office of the Director of National Intelligence.

(d) Mission

The mission of the National Counterintelligence and Security Center shall include organizing and leading strategic planning for counterintelligence activities of the United States Government by integrating instruments of national power as needed to counter foreign intelligence activities.

(e) Functions

Subject to the direction and control of the Director of the National Counterintelligence and Security Center, the functions of the National Counterintelligence and Security Center shall be as follows:

(1) National threat identification and prioritization assessment

Subject to subsection (f), in consultation with appropriate department and agencies of the United States Government, and private sector entities, to produce a strategic planning assessment of the counterintelligence requirements of the United States to be known as the National Threat Identification and Prioritization Assessment.

(2) National Counterintelligence Strategy

(A) Requirement to produce

Subject to subsection (f), in consultation with appropriate department and agencies of the United States Government, and private sector entities, and based on the most current National Threat Identification and Prioritization Assessment under paragraph (1), to produce a strategy for the counterintelligence programs and activities of the United States Government to be known as the National Counterintelligence Strategy.

(B) Revision and requirement

The National Counterintelligence Strategy shall be revised or updated at least once every three years and shall be aligned with the strategy and policies of the Director of National Intelligence.

(3) Implementation of National Counterintelligence Strategy

To evaluate on an ongoing basis the implementation of the National Counterintelligence Strategy and to submit to the President periodic reports on such evaluation, including a discussion of any shortfalls in the implementation of the Strategy and recommendations for remedies for such shortfalls.

(4) National counterintelligence strategic analyses

As directed by the Director of National Intelligence and in consultation with appropriate elements of the departments and agen-

cies of the United States Government, to oversee and coordinate the production of strategic analyses of counterintelligence matters, including the production of counterintelligence damage assessments and assessments of lessons learned from counterintelligence activities.

(5) National counterintelligence program budget

At the direction of the Director of National Intelligence—

(A) to coordinate the development of budgets and resource allocation plans for the counterintelligence programs and activities of the Department of Defense, the Federal Bureau of Investigation, the Central Intelligence Agency, and other appropriate elements of the United States Government;

(B) to ensure that the budgets and resource allocation plans developed under subparagraph (A) address the objectives and priorities for counterintelligence under the National Counterintelligence Strategy; and

(C) to submit to the National Security Council periodic reports on the activities undertaken by the Office under subparagraphs (A) and (B).

(6) National counterintelligence collection and targeting coordination

To develop priorities for counterintelligence investigations and operations, and for collection of counterintelligence, for purposes of the National Counterintelligence Strategy, except that the National Counterintelligence and Security Center may not—

(A) carry out any counterintelligence investigations or operations; or

(B) establish its own contacts, or carry out its own activities, with foreign intelligence services.

(7) National counterintelligence outreach, watch, and warning

(A) Counterintelligence vulnerability assessments and surveys

To develop standards and criteria for counterintelligence risk assessments and surveys of the vulnerability of the United States to intelligence threats, including with respect to critical infrastructure and critical technologies, in order to identify the areas, programs, and activities that require protection from such threats.

(B) Outreach

To carry out and coordinate outreach programs and activities on counterintelligence to other elements of the United States Government, and the private sector, and to coordinate the dissemination to the public of warnings on intelligence threats to the United States.

(C) Research and development

To ensure that research and development programs and activities of the United States Government, and the private sector, direct attention to the needs of the counterintelligence community for technologies, products, and services.

(D) Training and professional development

To develop policies and standards for training and professional development of individuals engaged in counterintelligence activities and to manage the conduct of joint training exercises for such personnel.

(E) Vulnerabilities from foreign commercial spyware

(i) Consultation

In carrying out efforts to secure covered devices, to consult with the private sector of the United States and reputable third-party researchers to identify vulnerabilities from foreign commercial spyware (as defined in section 3232a(a) of this title) and maintain effective security measures for such devices.

(ii) Covered device defined

In this subparagraph, the term “covered device” means any electronic mobile device including smartphones, tablet computing devices, or laptop computing devices, that is issued by an element of the intelligence community for official use.

(f) Additional requirements regarding National Threat Identification and Prioritization Assessment and National Counterintelligence Strategy

(1) A National Threat Identification and Prioritization Assessment under subsection (e)(1), and any modification of such assessment, shall not go into effect until approved by the President.

(2) A National Counterintelligence Strategy under subsection (e)(2), and any modification of such strategy, shall not go into effect until approved by the President.

(3) The Director of the National Counterintelligence and Security Center shall submit to the congressional intelligence committees each National Threat Identification and Prioritization Assessment, or modification thereof, and each National Counterintelligence Strategy, or modification thereof, approved under this section.

(4) In this subsection, the term “congressional intelligence committees” means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(g) Personnel

(1) Personnel of the National Counterintelligence and Security Center may consist of personnel employed by the Center or personnel on detail from any other department, agency, or element of the Federal Government. Any such detail may be on a reimbursable or nonreimbursable basis, at the election of the head of the agency detailing such personnel.

(2) Notwithstanding section 104(d)¹ or any other provision of law limiting the period of the detail of personnel on a nonreimbursable basis, the detail of an officer or employee of United States or a member of the Armed Forces under paragraph (1) on a nonreimbursable basis may be for any period in excess of one year that the Di-

¹ See References in Text note below.

rector of the National Counterintelligence and Security Center and the head of the department, agency, or element concerned consider appropriate.

(h) Treatment of activities under certain administrative laws

The files of the National Counterintelligence and Security Center shall be treated as operational files of the Central Intelligence Agency for purposes of section 701 of the National Security Act of 1947 (50 U.S.C. 3141) to the extent such files meet criteria under subsection (b) of that section for treatment of files as operational files of an element of the Agency.

(i) Oversight by Congress

The location of the National Counterintelligence and Security Center within the Office of the Director of National Intelligence shall not be construed as affecting access by Congress, or any committee of Congress, to—

- (1) any information, document, record, or paper in the possession of the Center; or
- (2) any personnel of the Center.

(j) Construction

Nothing in this section shall be construed as affecting the authority of the Director of National Intelligence, the Secretary of Defense, the Secretary of State, the Attorney General, or the Director of the Federal Bureau of Investigation as provided or specified under the National Security Act of 1947 or under other provisions of law.

(Pub. L. 107–306, title IX, § 904, Nov. 27, 2002, 116 Stat. 2434; Pub. L. 108–458, title I, §§ 1071(g)(2)(B), 1072(d)(1)(C), Dec. 17, 2004, 118 Stat. 3691, 3693; Pub. L. 111–259, title IV, § 412, Oct. 7, 2010, 124 Stat. 2725; Pub. L. 112–18, title IV, § 401, June 8, 2011, 125 Stat. 227; Pub. L. 112–87, title III, § 311(b), Jan. 3, 2012, 125 Stat. 1886; Pub. L. 115–31, div. N, title IV, § 401(b)(1)–(5), May 5, 2017, 131 Stat. 817, 818; Pub. L. 117–263, div. F, title LXIII, § 6318(d)(4), Dec. 23, 2022, 136 Stat. 3521; Pub. L. 118–31, div. G, title III, §§ 7303, 7305(a), (b)(1), Dec. 22, 2023, 137 Stat. 1025, 1026; Pub. L. 118–159, div. F, title LXIII, § 6302, Dec. 23, 2024, 138 Stat. 2471.)

Editorial Notes

REFERENCES IN TEXT

Section 104(d), referred to in subsec. (g)(2), is section 104(d) of Pub. L. 107–306, title I, Nov. 27, 2002, 116 Stat. 2387, which is not classified to the Code.

The National Security Act of 1947, referred to in subsec. (j), is act July 26, 1947, ch. 343, 61 Stat. 495, which is classified principally to chapter 44 (§ 3001 et seq.) of this title. For complete classification of this Act to the Code, see Tables.

CODIFICATION

Section was formerly classified to section 402c of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2024—Subsec. (f)(3). Pub. L. 118–159 substituted “Director of the National Counterintelligence and Security Center” for “National Counterintelligence Executive”.

2023—Subsec. (d). Pub. L. 118–31, § 7305(a)(2), added subsec. (d). Former subsec. (d) redesignated (e).

Subsec. (d)(7)(A). Pub. L. 118–31, § 7303, amended subpar. (A) generally. Prior to amendment, text read as follows: “To carry out and coordinate surveys of the vulnerability of the United States Government, and the private sector, to intelligence threats in order to identify the areas, programs, and activities that require protection from such threats.”

Subsec. (e). Pub. L. 118–31, § 7305(a)(1), (b)(1)(A), redesignated subsec. (d) as (e) and substituted “Subject to subsection (f)” for “Subject to subsection (e)” in pars. (1) and (2)(A). Former subsec. (e) redesignated (f).

Subsec. (f). Pub. L. 118–31, § 7305(a)(1), (b)(1)(B), redesignated subsec. (e) as (f) and substituted “subsection (e)(1)” for “subsection (d)(1)” in par. (1) and “subsection (e)(2)” for “subsection (d)(2)” in par. (2). Former subsec. (f) redesignated (g).

Subsecs. (g) to (j). Pub. L. 118–31, § 7305(a)(1), redesignated subsecs. (f) to (i) as (g) to (j), respectively.

2022—Subsec. (d)(7)(E). Pub. L. 117–263 added subpar. (E).

2017—Pub. L. 115–31, § 401(b)(1)(A), substituted “National Counterintelligence and Security Center” for “Office of the National Counterintelligence Executive” in section catchline.

Subsecs. (a) to (c). Pub. L. 115–31, § 401(b)(1)(B), added subsecs. (a) to (c) and struck out former subsecs. (a) to (c) which related to establishment of Office of the National Counterintelligence Executive, head of Office, and location of Office, respectively.

Subsec. (d). Pub. L. 115–31, § 401(b)(2)(A), substituted “Director of the National Counterintelligence and Security Center, the functions of the National Counterintelligence and Security Center” for “National Counterintelligence Executive, the functions of the Office of the National Counterintelligence Executive” in introductory provisions.

Subsec. (d)(5). Pub. L. 115–31, § 401(b)(2)(B), substituted “At the direction of” for “In consultation with” in introductory provisions.

Subsec. (d)(6). Pub. L. 115–31, § 401(b)(2)(C), substituted “National Counterintelligence and Security Center” for “Office” in introductory provisions.

Subsec. (f)(1). Pub. L. 115–31, § 401(b)(3)(A), substituted “National Counterintelligence and Security Center may consist of personnel employed by the Center” for “Office of the National Counterintelligence Executive may consist of personnel employed by the Office”.

Subsec. (f)(2). Pub. L. 115–31, § 401(b)(3)(B), substituted “Director of the National Counterintelligence and Security Center” for “National Counterintelligence Executive”.

Subsec. (g). Pub. L. 115–31, § 401(b)(4), substituted “National Counterintelligence and Security Center shall be treated as operational files of the Central Intelligence Agency for purposes of section 701 of the National Security Act of 1947 (50 U.S.C. 3141)” for “Office shall be treated as operational files of the Central Intelligence Agency for purposes of section 701 of the National Security Act of 1947 (50 U.S.C. 431)”.

Subsec. (h). Pub. L. 115–31, § 401(b)(5)(A), substituted “National Counterintelligence and Security Center” for “Office of the National Counterintelligence Executive” in introductory provisions.

Subsec. (h)(1), (2). Pub. L. 115–31, § 401(b)(5)(B), substituted “Center” for “Office”.

2012—Subsec. (d)(1). Pub. L. 112–87 struck out “on an annual basis” after “to produce”.

2011—Subsec. (d)(2). Pub. L. 112–18 inserted subpar. (A) designation and heading, struck out “on an annual basis” after “to produce”, and added subpar. (B).

2010—Subsec. (d). Pub. L. 111–259, § 412(a)(1), (2), redesignated subsec. (e) as (d) and struck out former subsec. (d). Text read as follows:

“(1) There shall be in the Office of the National Counterintelligence Executive a general counsel who shall serve as principal legal advisor to the National Counterintelligence Executive.

“(2) The general counsel shall—

“(A) provide legal advice and counsel to the Executive on matters relating to functions of the Office;

“(B) ensure that the Office complies with all applicable laws, regulations, Executive orders, and guidelines; and

“(C) carry out such other duties as the Executive may specify.”

Subsec. (d)(1), (2). Pub. L. 111-259, §412(b)(1), substituted “subsection (e)” for “subsection (f)”.

Subsec. (e). Pub. L. 111-259, §412(a)(2), redesignated subsec. (f) as (e). Former subsec. (e) redesignated (d).

Subsec. (e)(1). Pub. L. 111-259, §412(b)(2)(A), substituted “subsection (d)(1)” for “subsection (e)(1)”.

Subsec. (e)(2). Pub. L. 111-259, §412(b)(2)(B), substituted “subsection (d)(2)” for “subsection (e)(2)”.

Subsec. (f). Pub. L. 111-259, §412(a)(2), redesignated subsec. (g) as (f). Former subsec. (f) redesignated (e).

Subsec. (f)(3), (4). Pub. L. 111-259, §412(a)(3), struck out pars. (3) and (4) which read as follows:

“(3) The employment of personnel by the Office, including the appointment, compensation and benefits, management, and separation of such personnel, shall be governed by the provisions of law on such matters with respect to the personnel of the Central Intelligence Agency, except that, for purposes of the applicability of such provisions of law to personnel of the Office, the National Counterintelligence Executive shall be treated as the head of the Office.

“(4) Positions in the Office shall be excepted service positions for purposes of title 5.”

Subsecs. (g) to (m). Pub. L. 111-259, §412(a)(1), (2), redesignated subsecs. (k) to (m) as (g) to (i), respectively, and struck out former subsecs. (h) to (j) which related to support, availability of funds for reimbursement, and contracts, respectively. Former subsec. (g) redesignated (f).

2004—Subsec. (c). Pub. L. 108-458, §1072(d)(1)(C)(i), substituted “Office of the Director of National Intelligence” for “Office of the Director of Central Intelligence”.

Subsec. (e)(4). Pub. L. 108-458, §1071(g)(2)(B)(i), substituted “Director of National Intelligence” for “Director of Central Intelligence”.

Subsec. (e)(5). Pub. L. 108-458, §1071(g)(2)(B)(ii), substituted “Director of National Intelligence” for “Director of Central Intelligence” in introductory provisions.

Subsec. (h)(1), (2). Pub. L. 108-458, §1071(g)(2)(B)(iii), substituted “Director of National Intelligence” for “Director of Central Intelligence”.

Subsec. (l). Pub. L. 108-458, §1072(d)(1)(C)(ii), substituted “Office of the Director of National Intelligence” for “Office of the Director of Central Intelligence” in introductory provisions.

Subsec. (m). Pub. L. 108-458, §1071(g)(2)(B)(iv), substituted “Director of National Intelligence” for “Director of Central Intelligence”.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108-458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108-458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108-458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

RULE OF CONSTRUCTION—NO ENHANCED AUTHORITIES

Nothing in amendment made by Pub. L. 117-263 to be construed as enhancing, or otherwise changing, the authorities of the intelligence community to target, collect, process, or disseminate information regarding United States Government personnel, see section 6318(e) of Pub. L. 117-263, set out as a note under section 3232a of this title.

§ 3384. Intelligence Community Counterintelligence Office at the Department of Agriculture

(a) Definitions

In this section:

(1) Department

The term “Department” means the Department of Agriculture.

(2) Secretary

The term “Secretary” means the Secretary of Agriculture.

(b) Omitted

(c) Establishment of Intelligence Community Counterintelligence Office

(1) Agreement with Secretary of Agriculture

The Director of National Intelligence, acting through the Director of the National Counterintelligence and Security Center, shall seek to enter into an agreement with the Secretary under which the Director of National Intelligence and the Secretary shall establish within the Department an office, which shall be known as the “Intelligence Community Counterintelligence Office”, in accordance with this section.

(2) Location

The Intelligence Community Counterintelligence Office established pursuant to this section shall be physically located within the headquarters of the Department and within reasonable proximity to the offices of the leadership of the Department.

(3) Security

The Director of the National Counterintelligence and Security Center shall be responsible for the protection of classified information and for the establishment and enforcement of all security-related controls within the Intelligence Community Counterintelligence Office.

(d) Personnel

(1) Director

(A) Appointment

There shall be at the head of the Intelligence Community Counterintelligence Office a Director who is appointed by the Director of National Intelligence. The Director of the Intelligence Community Counterintelligence Office shall—

(i) be supervised and subject to performance evaluations by the Director of the National Counterintelligence and Security Center, in consultation with the Secretary;

(ii) be an employee of the intelligence community with significant counterintelligence experience; and

(iii) serve for a period of 3 years.

(B) Responsibilities

The Director of the Intelligence Community Counterintelligence Office shall carry out the following responsibilities:

(i) Serving as the head of the Intelligence Community Counterintelligence

Office, with supervisory responsibility for the Intelligence Community Counterintelligence Office and any other personnel assigned to the Intelligence Community Counterintelligence Office.

(ii) Advising the Secretary on counterintelligence and intelligence information.

(iii) Ensuring that counterintelligence threat information and, as appropriate, finished intelligence on topics related to the functions of the Department, are provided to appropriate personnel of the department or agency without delay.

(iv) Ensuring critical intelligence relevant to the Secretary is requested and disseminated in a timely manner.

(v) Establishing, as appropriate, mechanisms for collaboration through which Department subject matter experts, including those without security clearances, can share information and expertise with the intelligence community.

(vi) Correlating and evaluating counterintelligence threats identified within intelligence community reporting, in coordination with the National Counterintelligence and Security Center, and providing appropriate dissemination of such intelligence to officials of the Department with a need-to-know.

(vii) Advising the Secretary on methods to improve the counterintelligence posture of the Department.

(viii) Where appropriate, supporting the Department's leadership in engaging with the National Security Council.

(ix) In coordination with the National Counterintelligence and Security Center, establishing counterintelligence partnerships to improve the counterintelligence defense of the Department.

(2) Deputy Director

There shall be within the Intelligence Community Counterintelligence Office a Deputy Director who is appointed by the Secretary, in coordination with the Director of National Intelligence. The Deputy Director shall—

(A) be supervised and subject to performance evaluations by the Secretary, in consultation with the Director of the National Counterintelligence and Security Center;

(B) be a current or former employee of the Department with significant experience within the Department; and

(C) serve at the pleasure of the Secretary.

(3) Other employees

(A) Joint duty assignment

There shall be within the Intelligence Community Counterintelligence Office such other employees as the Director of National Intelligence, in consultation with the Secretary, determines appropriate. Employment at the Intelligence Community Counterintelligence Office is an intelligence community joint duty assignment. A permanent change of station to the Intelligence Community Counterintelligence Office shall be for a period of not less than 2 years.

(B) Supervision

The Director of the Intelligence Community Counterintelligence Office shall be re-

sponsible for the supervision and management of employees assigned to the Intelligence Community Counterintelligence Office, including employees assigned by program elements of the intelligence community and other Federal departments and agencies, as appropriate.

(C) Joint duty or assigned personnel reimbursement

The Director of National Intelligence shall reimburse a program element of the intelligence community or a Federal department or agency for any permanent change of station employee assigned to the Intelligence Community Counterintelligence Office from amounts authorized to be appropriated for the Office of the Director of National Intelligence.

(D) Operation under authority of Director of National Intelligence

Employees assigned to the Intelligence Community Counterintelligence Office under this paragraph shall operate under the authorities of the Director of National Intelligence for the duration of their assignment or period of employment within the Intelligence Community Counterintelligence Office, except for temporary duty assignment employees.

(E) Incentive pay

(i) In general

An employee who accepts employment at the Intelligence Community Counterintelligence Office during the 120-day period after the date of the establishment of the Intelligence Community Counterintelligence Office shall receive an incentive payment, which shall be payable by the Director of National Intelligence, in an amount equal to 10 percent of the base annual pay of the employee. Such an employee who completes 2 years of service in the Intelligence Community Counterintelligence Office may receive an incentive payment in an amount equal to 10 percent of the base annual pay of the employee if the Director of the Intelligence Community Counterintelligence Office determines the performance of the employee is exceptional.

(ii) Eligibility

An employee is only eligible for an incentive payment under clause (i) if the employee enters into an agreement with the Director of National Intelligence to serve in the Intelligence Community Counterintelligence Office for a period of at least 2 years.

(e) Funding

To the extent and in such amounts as specifically provided in advance in appropriations Acts for the purposes detailed in this subsection, the Director of National Intelligence may expend such sums as are authorized within the National Intelligence Program of the Office of the Director of National Intelligence for—

(1) the renovation, furnishing, and equipping of a Federal building, as necessary, to meet

the security and operational requirements of the Intelligence Community Counterintelligence Office;

(2) the provision of connectivity to the Intelligence Community Counterintelligence Office to enable briefings, secure audio and video communications, and collaboration between employees of the Department and the intelligence community at the unclassified, secret, and top secret levels;

(3) the provision of other information technology systems and devices, such as computers, printers, and phones, for use by employees of the Intelligence Community Counterintelligence Office;

(4) the assignment of employees of the intelligence community to support the operation of the Intelligence Community Counterintelligence Office; and

(5) the provision of other personal services necessary for the operation of the Intelligence Community Counterintelligence Office.

(f) Deadline for establishment of the Intelligence Community Counterintelligence Office

(1) Establishment

Not later than January 1, 2025, the Director of National Intelligence shall seek to establish, in accordance with this section, the Intelligence Community Counterintelligence Office within the Department.

(2) Report

Not later than 180 days after December 22, 2023, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report on the plan to establish the Intelligence Community Counterintelligence Office required under paragraph (1). Such report shall include the costs and schedule associated with establishing the Intelligence Community Counterintelligence Office.

(Pub. L. 118–31, div. G, title III, § 7318, Dec. 22, 2023, 137 Stat. 1033.)

Editorial Notes

CODIFICATION

Section is comprised of section 7318 of Pub. L. 118–31. Subsec. (b) of section 7318 of Pub. L. 118–31 repealed section 415 of Pub. L. 117–103, formerly set out as a note under section 532 of Title 28, Judiciary and Judicial Procedure.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of “intelligence community” and “congressional intelligence committees” as used in this section, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.

§ 3385. Benjamin Tallmadge Institute as primary Central Intelligence Agency entity for education and training in counterintelligence

(a) In general

The Director of the Central Intelligence Agency shall maintain the Benjamin Tallmadge In-

stitute as the primary entity within the Central Intelligence Agency for education and training related to all aspects of counterintelligence.

(b) Responsibilities of Director

The Director of the Central Intelligence Agency shall—

(1) ensure the Institute is fully and properly organized and has the resources necessary to provide counterintelligence education and training for all career fields within the Agency, including specialized certifications for Agency counterintelligence personnel;

(2) develop appropriate certification courses that are designed to educate, train, and certify Agency personnel in—

(A) counterintelligence threats, insider threats, and other counterintelligence processes and issues;

(B) the conduct and support of counterintelligence inquiries and investigations;

(C) relevant skills necessary for coordination with Federal law enforcement; and

(D) any other skills as the Director determines necessary;

(3) identify and designate specific positions for which an individual shall be required to have a certification described in paragraph (2) prior to filling such a position; and

(4) develop necessary infrastructure and capacity to support the availability of courses under subsection (c) to increase participation by personnel from other components of the intelligence community in the courses offered by the Institute.

(c) Training and familiarization courses

(1) In general

The head of the Institute shall—

(A) develop training and familiarization courses at different classification levels, including courses at an unclassified level; and

(B) offer instruction in the courses developed under subparagraph (A) or make training curricula available to other intelligence community components, as appropriate, to support outreach efforts.

(2) Availability of courses

The training and familiarization courses developed under paragraph (1) shall be made available to any of the following that have a need and appropriate clearance, as determined by the Director of the National Counterintelligence and Security Center in consultation with the Director of the Central Intelligence Agency, for a general education on counterintelligence threats, briefings on specific topics, or other training related to counterintelligence:

(A) Federal departments and agencies that are not elements of the intelligence community.

(B) State, local, and Tribal governments.

(C) Private sector entities.

(D) Such other personnel and entities as appropriate.

(d) Baseline certification course

(1) In general

The Institute shall develop, in coordination with the National Counterintelligence and Se-

curity Center and the Defense Intelligence Agency, and implement a baseline certification course for all counterintelligence career professionals that aligns the minimum certification requirements of the course and the Defense Counterintelligence Agent Course of the Joint Counterintelligence Training Activity.

(2) Availability of course

The baseline certification course developed under paragraph (1) shall be made available, on a space-available basis, to all intelligence community professionals and appropriate personnel with appropriate security clearance from any other agency, committee, commission, office, or other establishment in the executive, legislative, or judicial branch of the Federal Government.

(Pub. L. 118–31, div. G, title III, §7334, Dec. 22, 2023, 137 Stat. 1046.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “intelligence community” as used in this section, see section 7002 of Pub. L. 118–31, set out as a note under section 3003 of this title.

CHAPTER 46—CENTRAL INTELLIGENCE AGENCY

Sec.	
3501.	Definitions.
3502.	Seal of office.
3503.	Procurement authorities.
3504.	Repealed.
3505.	Personnel allowances and benefits.
3506.	General authorities.
3506a.	Transformation of Central Intelligence Agency.
3507.	Protection of nature of Agency’s functions.
3508.	Admission of essential aliens; limitation on number.
3509.	Repealed.
3510.	Appropriations.
3510a.	Availability of appropriations for construction projects.
3510b.	Acquisition of critical skills.
3511.	Benefits available in event of the death of personnel.
3512.	Gifts, devises, and bequests.
3513.	Misuse of Agency name, initials, or seal.
3514.	Retirement equity for spouses of certain employees.
3515.	Security personnel at Agency installations.
3516.	Health benefits for certain former spouses of Central Intelligence Agency employees.
3517.	Inspector General for Agency.
3518.	Special annuity computation rules for certain employees’ service abroad.
3518a.	Portability of overseas service retirement benefit.
3519.	Special rules for disability retirement and death-in-service benefits with respect to certain employees.
3519a.	Separation pay program for voluntary separation from service.
3519b.	Special rules for certain individuals injured by reason of war, insurgency, hostile act, terrorist activities, or incidents designated by the Director.
3520.	General Counsel of Central Intelligence Agency.
3521.	Central services program.
3522.	Detail of employees.
3523.	Intelligence operations and cover enhancement authority.

Sec.	
3524.	Support for the Associate Director of the Central Intelligence Agency for Military Affairs.
3525.	Office of the Ombudsman for Analytic Objectivity.
3526.	Improvement of education in science, technology, engineering, arts, and mathematics.
3527.	Chaplain Corps and Chief of Chaplains.
3528.	Compensation and professional standards for certain medical officers.
3529.	Medical advisory board.
3530.	Office of wellness and workforce support.
3531.	Sexual assault and sexual harassment within the Agency.
3532.	Reporting and investigation of allegations of sexual assault and sexual harassment.
3533.	Special Victim Investigator.

§ 3501. Definitions

When used in this chapter, the term—

(1) “Agency” means the Central Intelligence Agency;

(2) “Director” means the Director of the Central Intelligence Agency; and

(3) “Government agency” means any executive department, commission, council, independent establishment, corporation wholly or partly owned by the United States which is an instrumentality of the United States, board, bureau, division, service, office, officer, authority, administration, or other establishment, in the executive branch of the Government.

(June 20, 1949, ch. 227, §1, 63 Stat. 208; Pub. L. 86–707, title V, §511(a)(3), (c)(1), Sept. 6, 1960, 74 Stat. 800, 801; Pub. L. 108–458, title I, §1077, Dec. 17, 2004, 118 Stat. 3695.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403a of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2004—Pub. L. 108–458 redesignated subsecs. (a) to (c) as pars. (1) to (3), respectively, and amended par. (2) generally. Prior to amendment, par. (2) read as follows: “‘Director’ means the Director of Central Intelligence;”.

1960—Subsec. (c). Pub. L. 86–707, §511(c)(1), substituted “Government.” for “Government; and”.

Subsec. (d). Pub. L. 86–707, §511(a)(3), repealed subsec. (d) which defined “continental United States”. See section 5921 of Title 5, Government Organization and Employees.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2004 AMENDMENT

For Determination by President that amendment by Pub. L. 108–458 take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of this title.

Amendment by Pub. L. 108–458 effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108–458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of this title.

SHORT TITLE

Act June 20, 1949, ch. 227, §10, formerly §12, 63 Stat. 213; renumbered §10, July 7, 1958, Pub. L. 85–507,