''(C) ANNUAL REPORTS.—The Inspector General shall submit, through the Secretary, to the Committees on Armed Services of the Senate and the House of Representatives annual reports presenting findings and recommendations regarding—

''(i) the effects of policies, programs, systems, and processes of the Department, regarding personnel, on diversity and inclusion in the Department; and

''(ii) the effectiveness of such policies, programs, systems, and processes in preventing and responding to supremacist, extremist, and criminal gang activity of a member of the Armed Forces.

''(D) OCCASIONAL REPORTS.—The Inspector General shall, from time to time, submit to the Secretary additional reports as the Inspector General may determine.

''(E) ONLINE PUBLICATION.—The Inspector General shall publish each report under this paragraph on a publicly accessible website consistent with the requirements of the Inspector General Act of 1978 ([former] 5 U.S.C. App.) [see 5 U.S.C. 401 et seq.]..[sic]

''(b) ESTABLISHMENT OF STANDARD POLICIES, PROCESSES, TRACKING MECHANISMS, AND REPORTING REQUIREMENTS FOR SUPREMACIST, EXTREMIST, AND CRIMINAL GANG ACTIVITY IN CERTAIN ARMED FORCES.—

''(1) IN GENERAL.—The Secretary of Defense shall establish policies, processes, and mechanisms, standard across the covered Armed Forces, that ensure that—

''(A) all allegations (and related information) that a member of a covered Armed Force has engaged in a prohibited activity, are referred to the Inspector General of the Department of Defense;

''(B) the Inspector General can document and track the referral, for purposes of an investigation or inquiry of an allegation described in paragraph (1), to—

''(i) a military criminal investigative organization;

''(ii) an inspector general;

''(iii) a military police or security police organization;

''(iv) a military commander;

''(v) another organization or official of the Department; or

''(vi) a civilian law enforcement organization or official;

''(C) the Inspector General can document and track the referral, to a military commander or other appropriate authority, of the final report of an investigation or inquiry described in subparagraph (B) for action;

''(D) the Inspector General can document the determination of whether a member described in subparagraph (A) engaged in prohibited activity;

''(E) the Inspector General can document whether a member of a covered Armed Force was subject to action (including judicial, disciplinary, adverse, or corrective administrative action) or no action, as the case may be, based on a determination described in subparagraph (D); and

''(F) the Inspector General can provide, or track the referral to a civilian law enforcement agency of, any information described in this paragraph.

''(2) REPORT.—Not later than December 1 of each year beginning after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall submit to the appropriate congressional committees a report on the policies, processes, and mechanisms implemented under paragraph (1). Each report shall include, with respect to the fiscal year preceding the date of the report, the following:

''(A) The total number of referrals received by the Inspector General under paragraph (1)(A);

''(B) The total number of investigations and inquiries conducted pursuant to a referral described in paragraph (1)(B);

''(C) The total number of members of a covered Armed Force who, on the basis of determinations described in paragraph (1)(D) that the members engaged in prohibited activity, were subject to action described in paragraph (1)(E), including—

''(i) court-martial,

''(ii) other criminal prosecution,

''(iii) non-judicial punishment under Article 15 of the Uniform Code of Military Justice [10 U.S.C. 815]; or

''(iv) administrative action, including involuntary discharge from the Armed Forces, a denial of reenlistment, or counseling.

''(D) The total number of members of a covered Armed Force described in paragraph (1)(A) who were not subject to action described in paragraph (1)(E), notwithstanding determinations described in paragraph (1)(D) that such members engaged in prohibited activity.

''(E) The total number of referrals described in paragraph (1)(F).

''(3) DEFINITIONS.—In this subsection:

''(A) The term 'appropriate congressional committees' means—

''(i) the Committee on the Judiciary and the Committee on Armed Services of the Senate; and

''(ii) the Committee on the Judiciary and the Committee on Armed Services of the House of Representatives.

''(B) The term 'covered Armed Force' means an Armed Force under the jurisdiction of the Secretary of a military department.

''(C) The term 'prohibited activity' means an activity prohibited under Department of Defense Instruction 1325.06, titled 'Handling Dissident and Protest Activities Among Members of the Armed Forces', or any successor instruction.''

[Pub. L. 117–81, § 549K, which directed amendment of section 554(a) of Pub. L. 116–283, set out above, by substituting ''ASSISTANT'' for ''DEPUTY'' in section heading, was executed by substituting ''ASSISTANT'' for ''DEPUTY'' in subsec. heading, to reflect the probable intent of Congress.]

§ 142. Chief Information Officer

(a) There is a Chief Information Officer of the Department of Defense, who shall be appointed by the President, by and with the advice and consent of the Senate, from among civilians who are qualified to serve as such officer.

(b)(1) The Chief Information Officer of the Department of Defense—

(A) is the Chief Information Officer of the Department of Defense for the purposes of sections 3506(a)(2) and 3544(a)(3) of title 44;

(B) has the responsibilities and duties specified in sections 11315 and 11319 of title 40;

(C) has the responsibilities specified for the Chief Information Officer in sections 2223(a) and 2224 of this title;

(D) exercises authority, direction, and control over the Activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information Systems Security Program;

(E) exercises authority, direction, and control over the Defense Information Systems Agency, or any successor organization;

(F) has the responsibilities for policy, oversight, guidance, and coordination for all Department of Defense matters related to electromagnetic spectrum, including coordination with other Federal and industry agencies, coordination for classified programs, and in coordination with the Under Secretary for Personnel and Readiness, policies related to spectrum management workforce;

(G) has the responsibilities for policy, oversight, and guidance for matters related to precision navigation and timing; and

(H) has the responsibilities for policy, oversight, and guidance for the architecture and programs related to the information technology, networking, information assurance, cybersecurity, and cyber capability architectures of the Department.

(2)(A) The Secretary of Defense, acting through the Under Secretary of Defense (Comptroller), shall require the Secretaries of the military departments and the heads of the Defense Agencies with responsibilities associated with any activity specified in paragraph (1) to transmit the proposed budget for such activities for a fiscal year and for the period covered by the future-years defense program submitted to Congress under section 221 of this title for that fiscal year to the Chief Information Officer for review under subparagraph (B) before submitting the proposed budget to the Under Secretary of Defense (Comptroller).

(B) The Chief Information Officer shall review each proposed budget transmitted under subparagraph (A) and, not later than January 31 of the year preceding the fiscal year for which the budget is proposed, shall submit to the Secretary of Defense a report containing the comments of the Chief Information Officer with respect to all such proposed budgets, together with the certification of the Chief Information Officer regarding whether each proposed budget is adequate.

(C) Not later than March 31 of each year, the Secretary of Defense shall submit to Congress a report specifying each proposed budget contained in the most-recent report submitted under subparagraph (B) that the Chief Information Officer did not certify to be adequate. The report of the Secretary shall include the following matters:

(i) A discussion of the actions that the Secretary proposes to take, together with any recommended legislation that the Secretary considers appropriate, to address the inadequacy of the proposed budgets specified in the report.

(ii) Any additional comments that the Secretary considers appropriate regarding the inadequacy of the proposed budgets.

(3)(A) The Secretary of a military department or head of a Defense Agency may not develop or procure information technology (as defined in section 11101 of title 40) that does not fully comply with such standards as the Chief Information Officer may establish.

(B) The Chief Information Officer shall implement and enforce a process for—

(i) developing, adopting, or publishing standards for information technology, networking, or cyber capabilities to which any military department or defense agency would need to adhere in order to run such capabilities on defense networks; and

(ii) certifying on a regular and ongoing basis that any capabilities being developed or procured meets such standards as have been published by the Department at the time of certification.

(C) The Chief Information Officer shall identify gaps in standards and mitigation plans for operating in the absence of acceptable standards.

(4) The Chief Information Officer shall perform such additional duties and exercise such powers as the Secretary of Defense may prescribe.

(c) The Chief Information Officer takes precedence in the Department of Defense with the officials serving in positions specified in section 131(b)(4) of this title. The officials serving in positions specified in section 131(b)(4) and the Chief Information Officer of the Department of Defense take precedence among themselves in the order prescribed by the Secretary of Defense.

(d) The Chief Information Officer of the Department of Defense shall report directly to the Secretary of Defense in the performance of duties under this section.

(Added and amended Pub. L. 113–291, div. A, title IX, §901(b)(1), (j)(1)(B), Dec. 19, 2014, 128 Stat. 3463, 3467; Pub. L. 114–328, div. A, title IX, §902(a), Dec. 23, 2016, 130 Stat. 2343; Pub. L. 115–91, div. A, title IX, §909(a)–(d), title X, §1081(b)(1)(A), Dec. 12, 2017, 131 Stat. 1514, 1515, 1597; Pub. L. 115–232, div. A, title IX, §903, Aug. 13, 2018, 132 Stat. 1922; Pub. L. 116–92, div. A, title IX, §903(a)(1), title XVI, §1662(b), Dec. 20, 2019, 133 Stat. 1555, 1772; Pub. L. 116–283, div. A, title X, §1081(a)(9), Jan. 1, 2021, 134 Stat. 3871; Pub. L. 117–81, div. A, title XV, §1523, Dec. 27, 2021, 135 Stat. 2042.)

Editorial Notes

PRIOR PROVISIONS

A prior section 142 of this title was renumbered section 138d of this title and subsequently repealed.

Another prior section 142 of this title was contained in chapter 5 of this title, prior to amendment by Pub. L. 99–433. See note preceding section 151 of this title.

AMENDMENTS

2021—Subsec. (b)(1)(A). Pub. L. 117–81, §1523(1), struck out ''(other than with respect to business management)'' after ''sections 3506(a)(2)''.

Subsec. (b)(1)(B). Pub. L. 117–81, §1523(1), struck out ''(other than with respect to business management)'' after ''title 40''.

Subsec. (b)(1)(C). Pub. L. 117–81, §1523(1), struck out ''(other than with respect to business management)'' after ''sections 2223(a)''.

Subsec. (b)(1)(D). Pub. L. 117–81, §1523(2), amended subpar. (D) generally. Prior to amendment, subpar. (D) read as follows: ''exercises authority, direction, and control over the Information Assurance Directorate of the National Security Agency;''.

Subsecs. (c), (d). Pub. L. 116–283 redesignated subsec. (c) relating to the direct report of the Chief Information Officer to the Secretary of Defense as (d) and struck out former subsec. (d) which read as follows: ''The Chief Information Officer of the Department of Defense takes precedence in the Department of Defense with the officials serving in positions specified in section 131(b)(4) of this title. The officials serving in positions specified in such section and the Chief Information Officer take precedence among themselves in the order prescribed by the Secretary of Defense.''

2019—Subsec. (b)(1)(A) to (C). Pub. L. 116–92, §903(a)(1), struck out ''systems and'' after ''business''.

Subsec. (b)(1)(G) to (I). Pub. L. 116–92, §1662(b), redesignated subpars. (H) and (I) as (G) and (H), respectively, and struck out former subpar. (G) which read as fol-

lows: ''has the responsibilities for policy, oversight, guidance, and coordination for nuclear command and control systems;''.

2018—Subsec. (b)(1)(A). Pub. L. 115–232, § 903(1), inserted ''(other than with respect to business systems and management)'' after ''sections 3506(a)(2)''.

Subsec. (b)(1)(B). Pub. L. 115–232, § 903(2), substituted ''sections 11315 and 11319 of title 40 (other than with respect to business systems and management)'' for ''section 11315 of title 40''.

Subsec. (b)(1)(C). Pub. L. 115–232, § 903(3), substituted ''sections 2223(a) (other than with respect to business systems and management) and 2224'' for ''sections 2222, 2223(a), and 2224''.

2017—Subsec. (a). Pub. L. 115–91, § 909(a), inserted before period at end '', who shall be appointed by the President, by and with the advice and consent of the Senate, from among civilians who are qualified to serve as such officer''.

Subsec. (b)(1)(I). Pub. L. 115–91, § 909(b), substituted ''the information technology, networking, information assurance, cybersecurity, and cyber capability architectures'' for ''the networking and cyber defense architecture''.

Subsec. (b)(2) to (4). Pub. L. 115–91, § 909(c), added pars. (2) and (3) and redesignated former par. (2) as (4).

Subsec. (c). Pub. L. 115–91, § 1081(b)(1)(A), repealed Pub. L. 113–291, § 901(j)(1)(B). See 2014 Amendment note below.

Pub. L. 115–91, § 909(d), added subsec. (c), relating to the direct report of the Chief Information Officer to the Secretary of Defense.

Subsec. (d). Pub. L. 115–91, § 909(d), added subsec. (d).

2016—Subsec. (b)(1)(E) to (I). Pub. L. 114–328 added subpars. (E) to (I).

2014—Subsec. (c). Pub. L. 113–291, § 901(j)(1)(B), which directed striking out subsec. (c), was repealed by Pub. L. 115–91, § 1081(b)(1)(A).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2017 AMENDMENT

Pub. L. 115–91, div. A, title IX, § 909(g), Dec. 12, 2017, 131 Stat. 1516, provided that: ''The amendments made by this section [amending this section] shall take effect on January 1, 2019.''

Pub. L. 115–91, div. A, title X, § 1081(b), Dec. 12, 2017, 131 Stat. 1597, provided that the amendment made by section 1081(b)(1)(A) is effective as of Dec. 23, 2016.

EFFECTIVE DATE OF 2014 AMENDMENT

Pub. L. 113–291, div. A, title IX, § 901(j)(1), Dec. 19, 2014, 128 Stat. 3467, which provided that the amendment made by section 901(j)(1)(B) is effective on the effective date specified in former section 901(a)(1) of Pub. L. 113–291, which was Feb. 1, 2017, was repealed by Pub. L. 115–91, div. A, title X, § 1081(b)(1)(A), Dec. 12, 2017, 131 Stat. 1597.

CRYPTOGRAPHIC MODERNIZATION SCHEDULES

Pub. L. 116–283, div. A, title I, § 153, Jan. 1, 2021, 134 Stat. 3442, provided that:

''(a) CRYPTOGRAPHIC MODERNIZATION SCHEDULES REQUIRED.—Each of the Secretaries of the military departments and the heads of relevant Defense Agencies and Department of Defense Field Activities shall establish and maintain a cryptographic modernization schedule that specifies, for each pertinent weapon system, command and control system, or data link under the jurisdiction of such Secretary or head, including those that use commercial encryption technologies (as relevant), the following:

''(1) The last year of use for applicable cryptographic algorithms.

''(2) Anticipated key extension requests for systems where cryptographic modernization is assessed to be overly burdensome and expensive or to provide limited operational utility.

''(3) The funding and deployment schedule for modernized cryptographic algorithms, keys, and equipment over the future-years defense program submitted to Congress pursuant to section 221 of title 10, United States Code, in 2021 together with the budget of the President for fiscal year 2022.

''(b) REQUIREMENTS FOR CHIEF INFORMATION OFFICER.—The Chief Information Officer of the Department of Defense shall—

''(1) oversee the construction and implementation of the cryptographic modernization schedules required by subsection (a);

''(2) establish and maintain an integrated cryptographic modernization schedule for the entire Department of Defense, collating the cryptographic modernization schedules required under subsection (a); and

''(3) in coordination with the Director of the National Security Agency and the Joint Staff Director for Command, Control, Communications, and Computers/Cyber, use the budget certification, standard-setting, and policy-making authorities provided in section 142 of title 10, United States Code, to amend Armed Force and Defense Agency and Field Activity plans for key extension requests and cryptographic modernization funding and deployment that pose unacceptable risk to military operations.

''(c) ANNUAL NOTICES.—Not later than January 1, 2022, and not less frequently than once each year thereafter until January 1, 2026, the Chief Information Officer and the Joint Staff Director shall jointly submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] notification of all—

''(1) delays to or planned delays of Armed Force and Defense Agency and Field Activity funding and deployment of modernized cryptographic algorithms, keys, and equipment over the previous year; and

''(2) changes in plans or schedules surrounding key extension requests and waivers, including—

''(A) unscheduled or unanticipated key extension requests; and

''(B) unscheduled or unanticipated waivers and nonwaivers of scheduled or anticipated key extension requests.''

SERVICE OF INCUMBENT WITHOUT FURTHER APPOINTMENT

Pub. L. 115–91, div. A, title IX, § 909(f), Dec. 12, 2017, 131 Stat. 1516, provided that: ''The individual serving in the position of Chief Information Officer of the Department of Defense as of January 1, 2019, may continue to serve in such position commencing as of that date without further appointment pursuant to section 142 of title 10, United States Code, as amended by this section.''

§ 143. Office of the Secretary of Defense personnel: limitation

(a) PERMANENT LIMITATION ON OSD PERSONNEL.—The number of OSD personnel may not exceed 4,300.

(b) OSD PERSONNEL DEFINED.—For purposes of this section, the term ''OSD personnel'' means military and civilian personnel of the Department of Defense who are assigned to, or employed in, functions in the Office of the Secretary of Defense (including Direct Support Activities of that Office and the Washington Headquarters Services of the Department of Defense).

(c) LIMITATION ON REASSIGNMENT OF FUNCTIONS.—In carrying out reductions in the number of personnel assigned to, or employed in, the Office of the Secretary of Defense in order to comply with this section, the Secretary of Defense may not reassign functions solely in order to evade the requirements contained in this section.