1989—Pub. L. 101–189, div. A, title IX, §931(e)(2), Nov. 29, 1989, 103 Stat. 1535, substituted ''Cooperative Agreements'' for ''Acquisition and Cross-Servicing Agreements'' in item for chapter 138.

1988—Pub. L. 100–456, div. A, title III, §§342(a)(2), 344(b)(2), title VIII, §821(b)(2), Sept. 29, 1988, 102 Stat. 1961, 1962, 2016, substituted ''Defense Industrial Base'' for ''Buy American Requirements'' in item for chapter 148, substituted ''Property Records and Report of Theft or Loss of Certain Property'' for ''Property Records'' in item for chapter 161, and added item for chapter 171.

Pub. L. 100–370, §§1(e)(2), 2(a)(2), 3(a)(2), July 19, 1988, 102 Stat. 845, 854, 855, added items for chapters 134, 146, and 148.

1987—Pub. L. 100–26, §7(c)(1), Apr. 21, 1987, 101 Stat. 280, substituted ''Acquisition and Cross-Servicing Agreements with NATO Allies and Other Countries'' for ''North Atlantic Treaty Organization Acquisition and Cross-Servicing Agreements'' in item for chapter 138, substituted ''Major Defense Acquisition Programs'' for ''Oversight of Cost Growth in Major Programs'' and ''2430'' for ''2431'' in item for chapter 144, and substituted ''2721'' for ''2701'' in item for chapter 161.

1986—Pub. L. 99–661, div. A, title XIII, §1343(a)(22), Nov. 14, 1986, 100 Stat. 3994, substituted ''2341'' for ''2321'' in item for chapter 138.

Pub. L. 99–499, title II, §211(a)(2), Oct. 17, 1986, 100 Stat. 1725, added item for chapter 160.

Pub. L. 99–433, title VI, §605(b), Oct. 1, 1986, 100 Stat. 1075a, added item for chapter 144.

1984—Pub. L. 98–525, title XII, §1241(a)(2), Oct. 19, 1984, 98 Stat. 2606, added item for chapter 142.

1982—Pub. L. 97–295, §1(50)(E), Oct. 12, 1982, 96 Stat. 1300, added item for chapter 167.

Pub. L. 97–214, §2(b), July 12, 1982, 96 Stat. 169, added item for chapter 169.

1980—Pub. L. 96–323, §2(b), Aug. 4, 1980, 94 Stat. 1019, added item for chapter 138.

CHAPTER 131—PLANNING AND COORDINATION

Sec.
2201. Apportionment of funds: authority for exemption; excepted expenses.
2202. Regulations on production, warehousing, and supply distribution functions.
2203. Budget estimates.
2204. Obligation of appropriations.
2205. Reimbursements.
2206. Disbursement of funds of military department to cover obligation of another agency of Department of Defense.
2207. Expenditure of appropriations: limitation.[1]
2208. Working-capital funds.
2209. Management funds.
2210. Proceeds of sales of supplies: credit to appropriations.
2211. Reimbursement for equipment, material, or services furnished members of the United Nations.
[2212, 2213. Renumbered.]
2214. Transfer of funds: procedure and limitations.
2215. Transfer of funds to other departments and agencies: limitation.
[2216. Renumbered.]
2216a. Rapidly meeting urgent needs: Joint Urgent Operational Needs Fund.
[2217. Renumbered.]
2218. National Defense Sealift Fund.
2218a. National Sea-Based Deterrence Fund.
2219. Grants for improvement of Navy ship repair or alterations capability.
2220. Performance based management: acquisition programs.
[2221. Repealed.]
2222. Defense business systems: business process reengineering; enterprise architecture; management.
2223. Information technology: additional responsibilities of Chief Information Officers.
2223a. Information technology acquisition planning and oversight requirements.[1]
2224. Defense Information Assurance Program.
2224a. Information security: continued applicability of expiring Governmentwide requirements to the Department of Defense.
[2225. Repealed.]
2226. Contracted property and services: prompt payment of vouchers.[1]
2227. Electronic submission and processing of claims for contract payments.[1]
2228. Office of Corrosion Policy and Oversight.
2229. Strategic policy on prepositioning of materiel and equipment.
2229a. Annual report on prepositioned materiel and equipment.
[2229b. Renumbered.]

Editorial Notes

AMENDMENTS

2023—Pub. L. 118–31, div. A, title X, §1017, Dec. 22, 2023, 137 Stat. 382, added item 2219. Amendment was made pursuant to operation of section 102 of this title.

2021—Pub. L. 116–283, div. A, title XVIII, §§1807(b)(2)(B), (g)(2), 1809(f)(2), (g)(2), (i)(2), Jan. 1, 2021, 134 Stat. 4157, 4159, 4161, 4162, substituted ''Regulations on production, warehousing, and supply distribution functions'' for ''Regulations on procurement, production, warehousing, and supply distribution functions'' in item 2202 and struck out items 2212 ''Obligations for contract services: reporting in budget object classes'', 2213 ''Limitation on acquisition of excess supplies'', 2216 ''Defense Modernization Account'', 2217 ''Comparable budgeting for common procurement weapon systems'', and 2229b ''Comptroller General assessment of acquisition programs and initiatives''.

2019—Pub. L. 116–92, div. A, title XVII, §1731(a)(33), Dec. 20, 2019, 133 Stat. 1814, substituted ''Comptroller General assessment of acquisition programs and initiatives'' for ''Comptroller General assessment of acquisition programs and related initiatives'' in item 2229b.

2018—Pub. L. 115–232, div. A, title VIII, §833(b), Aug. 13, 2018, 132 Stat. 1859, added item 2229b.

2016—Pub. L. 114–328, div. A, title X, §1081(c)(4), Dec. 23, 2016, 130 Stat. 2419, made technical correction to directory language of Pub. L. 114–92, §883(a)(2). See 2015 Amendment note below.

Pub. L. 114–328, div. A, title VIII, §833(b)(2)(B), Dec. 23, 2016, 130 Stat. 2284, struck out item 2225 ''Information technology purchases: tracking and management''.

2015—Pub. L. 114–92, div. A, title VIII, §883(a)(2), Nov. 25, 2015, 129 Stat. 947, as amended by Pub. L. 114–328, div. A, title X, §1081(c)(4), Dec. 23, 2016, 130 Stat. 2419, added item 2222 and struck out former item 2222 ''Defense business systems: architecture, accountability, and modernization''.

2014—Pub. L. 113–291, div. A, title X, §1022(a)(2), Dec. 19, 2014, 128 Stat. 3487, added item 2218a.

2011—Pub. L. 112–81, div. A, title VIII, §846(a)(2), Dec. 31, 2011, 125 Stat. 1517, added item 2216a.

Pub. L. 111–383, div. A, title VIII, §805(a)(2), Jan. 7, 2011, 124 Stat. 4259, added item 2223a.

2008—Pub. L. 110–181, div. A, title III, §§352(b), 371(f), Jan. 28, 2008, 122 Stat. 72, 81, added items 2228 and 2229a and struck out former item 2228 ''Military equipment and infrastructure: prevention and mitigation of corrosion''.

2006—Pub. L. 109–364, div. A, title III, §351(b), Oct. 17, 2006, 120 Stat. 2160, added item 2229.

2004—Pub. L. 108–375, div. A, title III, §332(a)(2), title VI, §651(f)(2), Oct. 28, 2004, 118 Stat. 1854, 1972, struck out item 2219 ''Retention of morale, welfare, and recreation funds by military installations: limitation'' and added item 2222.

2002—Pub. L. 107–314, div. A, title X, §§1004(h)(1), 1052(b)(2), 1067(a)(2), Dec. 2, 2002, 116 Stat. 2631, 2649,

[1] Section renumbered by Pub. L. 116–283 without corresponding amendment of chapter analysis.

2658, struck out item 2222 ''Annual financial management improvement plan'' and added items 2224a and 2228.

2001—Pub. L. 107–107, div. A, title X, §1009(b)(3)(B), Dec. 28, 2001, 115 Stat. 1209, substituted ''Annual'' for ''Biennial'' in item 2222.

2000—Pub. L. 106–398, §1 [[div. A], title VIII, §812(a)(2), title X, §§1006(a)(2), 1008(a)(2)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, 1654A–247, 1654A–250, added items 2225, 2226, and 2227.

1999—Pub. L. 106–65, div. A, title X, §1043(b), Oct. 5, 1999, 113 Stat. 761, added item 2224.

1998—Pub. L. 105–261, div. A, title III, §331(a)(2), title IX, §§906(f)(1), 911(a)(2), title X, §1008(b), Oct. 17, 1998, 112 Stat. 1968, 2096, 2099, 2117, added item 2212, struck out items 2216a ''Defense Business Operations Fund'' and 2221 ''Fisher House trust funds'', and added item 2223.

1997—Pub. L. 105–85, div. A, title X, §1008(a)(2), Nov. 18, 1997, 111 Stat. 1871, added item 2222.

1996—Pub. L. 104–201, div. A, title X, §1074(a)(10), Sept. 23, 1996, 110 Stat. 2659, redesignated item 2216 ''Defense Business Operations Fund'' as 2216a.

Pub. L. 104–106, div. A, title III, §371(a)(2), title IX, §§912(a)(2), 914(a)(2), Feb. 10, 1996, 110 Stat. 279, 410, 412, added two items 2216 and item 2221.

1994—Pub. L. 103–355, title II, §2454(c)(3)(A), title III, §3061(b), title V, §5001(a)(2), Oct. 13, 1994, 108 Stat. 3326, 3336, 3350, substituted ''Regulations on procurement, production, warehousing, and supply distribution functions'' for ''Obligation of funds: limitation'' in item 2202, struck out item 2212 ''Contracted advisory and assistance services: accounting procedures'', and added item 2220.

Pub. L. 103–337, div. A, title III, §373(b), div. B, title XXVIII, §2804(b)(2), Oct. 5, 1994, 108 Stat. 2736, 3053, substituted ''Reimbursements'' for ''Availability of reimbursements'' in item 2205 and added item 2219.

1993—Pub. L. 103–160, div. A, title XI, §1106(a)(2), Nov. 30, 1993, 107 Stat. 1750, added item 2215.

1992—Pub. L. 102–484, div. A, title X, §1024(a)(2), Oct. 23, 1992, 106 Stat. 2488, added item 2218.

1991—Pub. L. 102–190, div. A, title III, §317(b), Dec. 5, 1991, 105 Stat. 1338, added item 2213.

1990—Pub. L. 101–510, div. A, title XIII, §1331(2), title XIV, §§1482(c)(2), 1484(i)(6), Nov. 5, 1990, 104 Stat. 1673, 1710, 1718, struck out item 2213 ''Cooperative military airlift agreements'', added item 2214, and struck out items 2215 ''Reports on unobligated balances'' and 2216 ''Annual report on budgeting for inflation''.

1988—Pub. L. 100–370, §1(d)(4), July 19, 1988, 102 Stat. 843, added items 2201, 2212, and 2217.

1986—Pub. L. 99–661, div. A, title XIII, §1307(a)(2), Nov. 14, 1986, 100 Stat. 3981, added items 2215 and 2216.

1982—Pub. L. 97–252, title XI, §1125(b), Sept. 8, 1982, 96 Stat. 758, added item 2213.

Pub. L. 97–214, §10(a)(1), July 12, 1982, 96 Stat. 174, struck out item 2212 ''Transmission of annual military construction authorization request''.

1978—Pub. L. 95–356, title VIII, §802(a)(2), Sept. 8, 1978, 92 Stat. 585, added item 2212.

1962—Pub. L. 87–651, title II, §207(b), Sept. 7, 1962, 76 Stat. 523, added items 2203 to 2211.

1958—Pub. L. 85–599, §3(c), Aug. 6, 1958, 72 Stat. 516, struck out item 2201 ''General functions of Secretary of Defense''.

Statutory Notes and Related Subsidiaries

MISSION INTEGRATION MANAGEMENT

Pub. L. 114–328, div. A, title VIII, §855, Dec. 23, 2016, 130 Stat. 2297, directed the Secretary of Defense to establish mission integration management activities for certain mission areas that involve multiple Armed Forces and multiple programs and to submit to the congressional defense committees, at the same time the fiscal year 2018 budget is submitted to Congress, a strategy for mission integration management.

STRATEGIC MANAGEMENT PLAN

Pub. L. 110–181, div. A, title IX, §904(d), (e), Jan. 28, 2008, 122 Stat. 275, as amended by Pub. L. 114–92, div. A, title X, §1079(e), Nov. 25, 2015, 129 Stat. 999, provided that:

''(d) STRATEGIC MANAGEMENT PLAN REQUIRED.—

''(1) REQUIREMENT.—The Secretary of Defense, acting through the Chief Management Officer of the Department of Defense, shall develop a strategic management plan for the Department of Defense.

''(2) MATTERS COVERED.—Such plan shall include, at a minimum, detailed descriptions of—

''(A) performance goals and measures for improving and evaluating the overall efficiency and effectiveness of the business operations of the Department of Defense and achieving an integrated management system for business support areas within the Department of Defense;

''(B) key initiatives to be undertaken by the Department of Defense to achieve the performance goals under subparagraph (A), together with related resource needs;

''(C) procedures to monitor the progress of the Department of Defense in meeting performance goals and measures under subparagraph (A);

''(D) procedures to review and approve plans and budgets for changes in business operations, including any proposed changes to policies, procedures, processes, and systems, to ensure the compatibility of such plans and budgets with the strategic management plan of the Department of Defense; and

''(E) procedures to oversee the development of, and review and approve, all budget requests for defense business systems.

''(e) REPORT.—Not later than 180 days after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense shall provide to the Committees on Armed Services of the Senate and the House of Representatives a report on the implementation of this section and a copy of the strategic management plan required by subsection (d).''

§ 2201. Apportionment of funds: authority for exemption; excepted expenses

(a) EXEMPTION FROM APPORTIONMENT REQUIREMENT.—If the President determines such action to be necessary in the interest of national defense, the President may exempt from the provisions of section 1512 of title 31 appropriations, funds, and contract authorizations available for military functions of the Department of Defense.

(b) AIRBORNE ALERTS.—Upon a determination by the President that such action is necessary, the Secretary of Defense may provide for the cost of an airborne alert as an excepted expense under section 6301(a) and (b)(1)–(3) of title 41.

(c) MEMBERS ON ACTIVE DUTY.—Upon a determination by the President that it is necessary to increase (subject to limits imposed by law) the number of members of the armed forces on active duty beyond the number for which funds are provided in appropriation Acts for the Department of Defense, the Secretary of Defense may provide for the cost of such additional members as an excepted expense under section 6301(a) and (b)(1)–(3) of title 41.

(d) NOTIFICATION TO CONGRESS.—The Secretary of Defense shall immediately notify Congress of the use of any authority under this section.

(Added Pub. L. 100–370, §1(d)(1)(A), July 19, 1988, 102 Stat. 841; amended Pub. L. 106–65, div. A, title X, §1032(a)(1), Oct. 5, 1999, 113 Stat. 751; Pub. L. 111–350, §5(b)(4), Jan. 4, 2011, 124 Stat. 3842.)

HISTORICAL AND REVISION NOTES

Section is based on Pub. L. 99–190, §101(b) [title VIII, §8009], Dec. 19, 1985, 99 Stat. 1185, 1204.

In two instances, the source law to be codified by the bill includes provisions that on their face require that the Department of Defense notify Congress of certain actions. These notification requirements were terminated by section 602 of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99–433), which terminated all recurring reporting requirements applicable to the Department of Defense except for those requirements that were specifically exempted in that section. The source law sections are sections 8009(c) and 8005(j) (proviso) of the FY86 defense appropriations Act (Public Law 99–190), enacted December 19, 1985, which would be codified as section 2201 of title 10 (by section 1(d) of the bill) and section 7313(a) of title 10 (by section 1(n) of the bill). In codifying the authorities provided the Department of Defense by these two provisions of law, the committee believes that it is appropriate to reinstate the congressional notification requirements that go with those authorities. These sections were recurring annual appropriation provisions for many years and were made permanent only months before the enactment of the 1986 Reorganization Act. It is the committee's belief that the failure to exempt these provisions from the general reports termination provision was inadvertent and notes that the notification provisions had in fact previously applied to the Department of Defense for many years. The action of the committee restores the status quo as it existed before the Reorganization Act.

Editorial Notes

PRIOR PROVISIONS

A prior section 2201, act Aug. 10, 1956, ch. 1041, 70A Stat. 119, prescribed the general functions of the Secretary of Defense, prior to repeal by Pub. L. 85–599, § 3(c), Aug. 6, 1958, 72 Stat. 516. See section 113 of this title.

AMENDMENTS

2011—Subsec. (b). Pub. L. 111–350, § 5(b)(4)(A), substituted ''section 6301(a) and (b)(1)–(3) of title 41'' for ''section 3732(a) of the Revised Statutes (41 U.S.C. 11(a))''.

Subsec. (c). Pub. L. 111–350, § 5(b)(4)(B), substituted ''section 6301(a) and (b)(1)–(3) of title 41'' for ''section 3732(a) of the Revised Statutes (41 U.S.C. 11(a))''.

1999—Subsec. (d). Pub. L. 106–65 substituted ''Defense'' for ''Defense—'', struck out par. (1) designation, substituted ''this section.'' for ''this section; and'', and struck out par. (2) which read as follows: ''shall submit monthly reports to Congress on the estimated obligations incurred pursuant to subsections (b) and (c).''

§ 2202. Regulations on production, warehousing, and supply distribution functions

The Secretary of Defense shall prescribe regulations governing the performance within the Department of Defense of the production, warehousing, and supply distribution functions, and related functions, of the Department of Defense.

(Aug. 10, 1956, ch. 1041, 70A Stat. 120; Pub. L. 100–180, div. A, title XII, § 1202, Dec. 4, 1987, 101 Stat. 1153; Pub. L. 103–355, title III, § 3061(a), Oct. 13, 1994, 108 Stat. 3336; Pub. L. 116–283, div. A, title XVIII, § 1807(b)(2), Jan. 1, 2021, 134 Stat. 4157.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2202	41:162.	July 10, 1952, ch. 630, § 638, 66 Stat. 537.

The words ''an officer or agency * * * may * * * only'' are substituted for the words ''no officer or agency * * * shall * * * except''. The word ''of'', before the words ''the Department'', is substituted for the words ''in or under''. The words ''under regulations prescribed'' are substituted for the words ''in accordance with regulations issued''. The words ''after the effective date of this section'' and 41:162(b) are omitted as executed. The words ''or equipment'' are omitted as covered by the definition of ''supplies'' in section 101(26) of this title.

Editorial Notes

AMENDMENTS

2021—Pub. L. 116–283 struck out ''procurement,'' before ''production,'' in section catchline and text.

1994—Pub. L. 103–355 amended heading and text generally. Prior to amendment, text read as follows:

''(a) Notwithstanding any other provision of law, an officer or agency of the Department of Defense may obligate funds for procuring, producing, warehousing, or distributing supplies, or for related functions of supply management, only under regulations prescribed by the Secretary of Defense. The purpose of this section is to achieve the efficient, economical, and practical operation of an integrated supply system to meet the needs of the military departments without duplicate or overlapping operations or functions.

''(b) Except as otherwise provided by law, the availability for obligation of funds appropriated for any program, project, or activity of the Department of Defense expires at the end of the three-year period beginning on the date that such funds initially become available for obligation unless before the end of such period the Secretary of Defense enters into a contract for such program, project, or activity.''

1987—Pub. L. 100–180 designated existing provisions as subsec. (a) and added subsec. (b).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2021 AMENDMENT

Amendment by Pub. L. 116–283 effective Jan. 1, 2022, with additional provisions for delayed implementation and applicability of existing law, see section 1801(d) of Pub. L. 116–283, set out as a note preceding section 3001 of this title.

EFFECTIVE DATE OF 1994 AMENDMENT

For effective date and applicability of amendment by Pub. L. 103–355, see section 10001 of Pub. L. 103–355, set out as a note under section 8752 of this title.

§ 2203. Budget estimates

To account for, and report, the cost of performance of readily identifiable functional programs and activities, with segregation of operating and capital programs, budget estimates of the Department of Defense shall be prepared, presented, and justified, where practicable, and authorized programs shall be administered, in such form and manner as the Secretary of Defense, subject to the authority and direction of the President, may prescribe. As far as practicable, budget estimates and authorized programs of the military departments shall be uniform and in readily comparable form. The budget for the Department of Defense submitted to Congress for each fiscal year shall include data projecting the effect of the appropriations requested for materiel readiness requirements. The Secretary of Defense shall provide that the budget justification documents for such budget include information on the number of employees of contractors estimated to be working on contracts of the Department of Defense during the

fiscal year for which the budget is submitted. Such information shall be set forth in terms of employee-years or such other measure as will be uniform and readily comparable with civilian personnel of the Department of Defense.

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 520; amended Pub. L. 97–295, § 1(21), Oct. 12, 1982, 96 Stat. 1290; Pub. L. 99–661, div. A, title III, § 311, Nov. 14, 1986, 100 Stat. 3851.)

HISTORICAL AND REVISION NOTES
1956 ACT

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2203	5:172b.	July 26, 1947, ch. 343, § 403; added Aug. 10, 1949, ch. 412, § 11 (5th and 6th pars.), 63 Stat. 586.

The word ''prescribe'' is substituted for the word ''determine''. 5 U.S.C. 172b(b) is omitted as executed.

1982 ACT

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2203 (last sentence).	10:2203 (note).	July 30, 1977, Pub. L. 95–79, § 812 (last sentence), 91 Stat. 336.

The words ''for fiscal year 1979'' are omitted as executed. The words ''for each fiscal year'' are substituted for ''subsequent fiscal years'' for consistency.

Editorial Notes

AMENDMENTS

1986—Pub. L. 99–661 inserted provisions that budget justification documents include information on number of employees estimated to be working during the fiscal year, such information to be set forth in terms of employee-years or other measure as is uniform and comparable with civilian personnel of the Department of Defense.

1982—Pub. L. 97–295 inserted provision requiring that the budget for the Department of Defense submitted annually to Congress include data projecting the effect of the appropriations requested for materiel readiness requirements.

Statutory Notes and Related Subsidiaries

PRESIDENTIAL RECOMMENDATIONS RESPECTING MODIFICATIONS IN CRUISE MISSILE PROGRAM

Pub. L. 95–184, title II, § 203, Nov. 15, 1977, 91 Stat. 1382, provided that in authorizing funds under that Act [Pub. L. 95–184], Congress was asserting its readiness to consider, in accordance with the processes set forth in the Congressional Budget and Impoundment Control Act of 1974 [2 U.S.C. 621 et seq.] and the Budget and Accounting Act, 1921 [31 U.S.C. 1101 et seq.], such modifications in the United States cruise missile programs as the President might recommend to facilitate either negotiation or agreement in arms limitation or reduction talks.

REPORT TO CONGRESSIONAL COMMITTEES ON MATERIAL READINESS REQUIREMENTS FOR ARMED FORCES

Pub. L. 95–79, title VIII, § 812, July 30, 1977, 91 Stat. 336, as amended by Pub. L. 97–295, § 6(b), Oct. 12, 1982, 96 Stat. 1314, directed Secretary of Defense to submit to Congress, not later than February 15, 1978, a report setting forth quantifiable and measurable material readiness requirements for the Armed Forces, including the Reserve components thereof, monthly readiness status of the Armed Forces, including the reserve components thereof, during fiscal year 1977, and any changes in such requirements and status projected for fiscal years 1978 and 1979 and in the five-year defense program, and to inform Congress of any subsequent changes in the aforementioned materiel readiness requirements and the reasons for such changes.

MODIFICATIONS IN UNITED STATES STRATEGIC ARMS PROGRAMS ON RECOMMENDATION OF PRESIDENT

Pub. L. 95–79, title VIII, § 813, July 30, 1977, 91 Stat. 337, provided that in authorizing procurement under section 101 of that Act and research and development under section 201 of that Act, Congress was asserting its readiness to consider, in accordance with the processes set forth in the Congressional Budget and Impoundment Control Act of 1974 [2 U.S.C. 621 et seq.] and the Budget and Accounting Act, 1921 [31 U.S.C. 1101 et seq.], such modifications in United States strategic arms programs as the President might recommend to facilitate either negotiation or agreement in the Strategic Arms Limitation Talks.

§ 2204. Obligation of appropriations

To prevent overdrafts and deficiencies in the fiscal year for which appropriations are made, appropriations made to the Department of Defense or to a military department, and reimbursements thereto, are available for obligation and expenditure only under scheduled rates of obligation, or changes thereto, that have been approved by the Secretary of Defense. This section does not prohibit the Department of Defense from incurring a deficiency that it has been authorized by law to incur.

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 520.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2204	5:172c.	July 26, 1947, ch. 343, § 404; added Aug. 10, 1949, ch. 412, § 11 (7th par.), 63 Stat. 587.

The words ''on and after the beginning of the next fiscal year following August 10, 1949,'' are omitted as executed. The last sentence is substituted for the proviso in 5 U.S.C. 172c.

§ 2205. Reimbursements

(a) AVAILABILITY OF REIMBURSEMENTS.—Reimbursements made to appropriations of the Department of Defense or a department or agency thereof under sections 1535 and 1536 of title 31, or other amounts paid by or on behalf of a department or agency of the Department of Defense to another department or agency of the Department of Defense, or by or on behalf of personnel of any department or organization, for services rendered or supplies furnished, may be credited to authorized accounts. Funds so credited are available for obligation for the same period as the funds in the account so credited. Such an account shall be accounted for as one fund on the books of the Department of the Treasury.

(b) FIXED RATE FOR REIMBURSEMENT FOR CERTAIN SERVICES.—The Secretary of Defense and the Secretaries of the military departments may charge a fixed rate for reimbursement of the costs of providing planning, supervision, administrative, or overhead services incident to any construction, maintenance, or repair project to real property or for providing facility services,

irrespective of the appropriation financing the project or facility services.

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 520; amended Pub. L. 96–513, title V, § 511(71), Dec. 12, 1980, 94 Stat. 2926; Pub. L. 97–258, § 3(b)(4), Sept. 13, 1982, 96 Stat. 1063; Pub. L. 103–337, div. B, title XXVIII, § 2804(a), (b)(1), Oct. 5, 1994, 108 Stat. 3053.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2205	5:172g.	July 26, 1947, ch. 343, § 408; added Aug. 10, 1949, ch. 412, § 11 (23d par.), 63 Stat. 590.

5 U.S.C. 172g is restated to reflect more clearly its purpose to authorize the Department of Defense to operate as an integrated department by permitting supplies to be furnished and services to be rendered within and among agencies of the Department of Defense and provide that reimbursements therefor be credited to authorized accounts and be available for the same purpose and period as the accounts so credited. (See Senate Report No. 366, 81st Congress, pp. 23, 24.)

Editorial Notes

AMENDMENTS

1994—Pub. L. 103–337 substituted ''Reimbursements'' for ''Availability of reimbursements'' as section catchline, designated existing provisions as subsec. (a) and inserted subsec. heading, and added subsec. (b).

1982—Pub. L. 97–258 substituted ''sections 1535 and 1536 of title 31'' for ''the Act of March 4, 1915 (31 U.S.C. 686)''.

1980—Pub. L. 96–513 substituted ''the Act of March 4, 1915 (31 U.S.C. 686)'' for ''section 686 of title 31''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 1980 AMENDMENT

Amendment by Pub. L. 96–513 effective Dec. 12, 1980, see section 701(b)(3) of Pub. L. 96–513, set out as a note under section 101 of this title.

§ 2206. Disbursement of funds of military department to cover obligation of another agency of Department of Defense

As far as authorized by the Secretary of Defense, a disbursing official of a military department may, out of available advances, make disbursements to cover obligations in connection with any function, power, or duty of another department or agency of the Department of Defense and charge those disbursements on vouchers, to the appropriate appropriation of that department or agency. Disbursements so made shall be adjusted in settling the accounts of the disbursing official.

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 520; amended Pub. L. 97–258, § 2(b)(1)(A), Sept. 13, 1982, 96 Stat. 1052.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2206	5:172h. 5:171n(a) (as applicable to 5:172h).	July 26, 1947, ch. 343, § 409; added Aug. 10, 1949, ch. 412, § 11 (24th par.), 63 Stat. 590. July 26, 1947, ch. 343, § 308(a) (as applicable to § 409), 61 Stat. 509.

The word ''agency'' is substituted for the word ''organization''. The last sentence is substituted for the proviso in 5 U.S.C. 172h.

Editorial Notes

AMENDMENTS

1982—Pub. L. 97–258 substituted ''official'' for ''officer'' wherever appearing.

[§ 2207. Renumbered § 4651]

§ 2208. Working-capital funds

(a) To control and account more effectively for the cost of programs and work performed in the Department of Defense, the Secretary of Defense may require the establishment of working-capital funds in the Department of Defense to—

(1) finance inventories of such supplies as he may designate; and

(2) provide working capital for such industrial-type activities, and such commercial-type activities that provide common services within or among departments and agencies of the Department of Defense, as he may designate.

(b) Upon the request of the Secretary of Defense, the Secretary of the Treasury shall establish working-capital funds established under this section on the books of the Department of the Treasury.

(c) Working-capital funds shall be charged, when appropriate, with the cost of—

(1) supplies that are procured or otherwise acquired, manufactured, repaired, issued, or used, including the cost of the procurement and qualification of technology-enhanced maintenance capabilities that improve either reliability, maintainability, sustainability, or supportability and have, at a minimum, been demonstrated to be functional in an actual system application or operational environment; and

(2) services or work performed;

including applicable administrative expenses, and be reimbursed from available appropriations or otherwise credited for those costs, including applicable administrative expenses and costs of using equipment.

(d) The Secretary of Defense may provide capital for working-capital funds by capitalizing inventories. In addition, such amounts may be appropriated for the purpose of providing capital for working-capital funds as have been specifically authorized by law.

(e) Subject to the authority and direction of the Secretary of Defense, the Secretary of each military department shall allocate responsibility for its functions, powers, and duties to accomplish the most economical and efficient organization and operation of the activities, and the most economical and efficient use of the inventories, for which working-capital funds are authorized by this section. The accomplishment of the most economical and efficient organization and operation of working capital fund activities for the purposes of this subsection shall include actions toward the following:

(1) Undertaking efforts to optimize the rate structure for all requisitioning entities.

(2) Encouraging a working capital fund activity to perform reimbursable work for other

entities to sustain the efficient use of the workforce.

(3) Determining the appropriate leadership level for approving work from outside entities to maximize efficiency.

(f) The requisitioning agency may not incur a cost for supplies drawn from inventories, or services or work performed by industrial-type or commercial-type activities for which working-capital funds may be established under this section, that is more than the amount of appropriations or other funds available for those purposes.

(g) The appraised value of supplies returned to working-capital funds by a department, activity, or agency may be charged to that fund. The proceeds thereof shall be credited to current applicable appropriations and are available for expenditure for the same purposes that those appropriations are so available. Credits may not be made to appropriations under this subsection as the result of capitalization of inventories under subsection (d).

(h) The Secretary of Defense shall prescribe regulations governing the operation of activities and use of inventories authorized by this section. The regulations may, if the needs of the Department of Defense require it and it is otherwise authorized by law, authorize supplies to be sold to, or services to be rendered or work performed for, persons outside the Department of Defense. However, supplies available in inventories financed by working capital funds established under this section may be sold to contractors for use in performing contracts with the Department of Defense. Working-capital funds shall be reimbursed for supplies so sold, services so rendered, or work so performed by charges to applicable appropriations or payments received in cash.

(i) For provisions relating to sales outside the Department of Defense of manufactured articles and services by a working-capital funded Army industrial facility (including a Department of the Army arsenal) that manufactures large caliber cannons, gun mounts, recoil mechanisms, ammunition, munitions, or components thereof, see section 7543 of this title.

(j)(1) The Secretary of a military department may authorize a working capital funded industrial facility of that department to manufacture or remanufacture articles and sell these articles, as well as manufacturing, remanufacturing, and engineering services provided by such facilities, to persons outside the Department of Defense if—

(A) the person purchasing the article or service is fulfilling a Department of Defense contract or a subcontract under a Department of Defense contract, and the solicitation for the contract or subcontract is open to competition between Department of Defense activities and private firms; or

(B) the Secretary would advance the objectives set forth in section 2474(b)(2) of this title by authorizing the facility to do so.

(2) The Secretary of Defense may waive the conditions in paragraph (1) in the case of a particular sale if the Secretary determines that the waiver is necessary for reasons of national security and notifies Congress regarding the reasons for the waiver.

(k)(1) Subject to paragraph (2), a contract for the procurement of a capital asset financed by a working-capital fund may be awarded in advance of the availability of funds in the working-capital fund for the procurement.

(2) Paragraph (1) applies to any of the following capital assets that have a development or acquisition cost of not less than $500,000 for procurements by a major range and test facility installation or a science and technology reinvention laboratory and not less than $250,000 for procurements at all other facilities:

(A) An unspecified minor military construction project under section 2805(c) of this title.

(B) Automatic data processing equipment or software.

(C) Any other equipment.

(D) Any other capital improvement.

(*l*)(1) An advance billing of a customer of a working-capital fund may be made if the Secretary of the military department concerned submits to Congress written notification of the advance billing within 30 days after the end of the month in which the advanced billing was made. The notification shall include the following:

(A) The reasons for the advance billing.

(B) An analysis of the effects of the advance billing on military readiness.

(C) An analysis of the effects of the advance billing on the customer.

(2) The Secretary of Defense may waive the notification requirements of paragraph (1)—

(A) during a period of war or national emergency; or

(B) to the extent that the Secretary determines necessary to support a contingency operation.

(3)(A) Except as provided in subparagraph (B), the total amount of the advance billings rendered or imposed for all working-capital funds of the Department of Defense in a fiscal year may not exceed $1,000,000,000.

(B) The dollar limitation under subparagraph (A) shall not apply with respect to advance billing for relief efforts following a declaration of a major disaster or emergency under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(4) This subsection shall not apply to advance billing for background investigation and related services performed by the Defense Counterintelligence and Security Agency.

(5) In this subsection:

(A) The term ''advance billing'', with respect to a working-capital fund, means a billing of a customer by the fund, or a requirement for a customer to reimburse or otherwise credit the fund, for the cost of goods or services provided (or for other expenses incurred) on behalf of the customer that is rendered or imposed before the customer receives the goods or before the services have been performed.

(B) The term ''customer'' means a requisitioning component or agency.

(m) CAPITAL ASSET SUBACCOUNTS.—Amounts charged for depreciation of capital assets shall

be credited to a separate capital asset subaccount established within a working-capital fund.

(n) SEPARATE ACCOUNTING, REPORTING, AND AUDITING OF FUNDS AND ACTIVITIES.—The Secretary of Defense, with respect to the working-capital funds of each Defense Agency, and the Secretary of each military department, with respect to the working-capital funds of the military department, shall provide for separate accounting, reporting, and auditing of funds and activities managed through the working-capital funds.

(*o*) CHARGES FOR GOODS AND SERVICES PROVIDED THROUGH THE FUND.—(1) Charges for goods and services provided for an activity through a working-capital fund shall include the following:

(A) Amounts necessary to recover the full costs of the goods and services provided for that activity.

(B) Amounts for depreciation of capital assets, set in accordance with generally accepted accounting principles.

(2) Charges for goods and services provided through a working-capital fund may not include the following:

(A) Amounts necessary to recover the costs of a military construction project (as defined in section 2801(b) of this title), other than a minor construction project financed by the fund pursuant to section 2805(c) of this title.

(B) Amounts necessary to cover costs incurred in connection with the closure or realignment of a military installation.

(C) Amounts necessary to recover the costs of functions designated by the Secretary of Defense as mission critical, such as ammunition handling safety, and amounts for ancillary tasks not directly related to the mission of the function or activity managed through the fund.

(p) PROCEDURES FOR ACCUMULATION OF FUNDS.—The Secretary of Defense, with respect to each working-capital fund of a Defense Agency, and the Secretary of a military department, with respect to each working-capital fund of the military department, shall establish billing procedures to ensure that the balance in that working-capital fund does not exceed the amount necessary to provide for the working-capital requirements of that fund, as determined by the Secretary.

(q) ANNUAL REPORTS AND BUDGET.—The Secretary of Defense, with respect to each working-capital fund of a Defense Agency, and the Secretary of each military department, with respect to each working-capital fund of the military department, shall annually submit to Congress, at the same time that the President submits the budget under section 1105 of title 31, the following:

(1) A detailed report that contains a statement of all receipts and disbursements of the fund (including such a statement for each subaccount of the fund) for the fiscal year ending in the year preceding the year in which the budget is submitted.

(2) A detailed proposed budget for the operation of the fund for the fiscal year for which the budget is submitted.

(3) A comparison of the amounts actually expended for the operation of the fund for the fiscal year referred to in paragraph (1) with the amount proposed for the operation of the fund for that fiscal year in the President's budget.

(4) A report on the capital asset subaccount of the fund that contains the following information:

(A) The opening balance of the subaccount as of the beginning of the fiscal year in which the report is submitted.

(B) The estimated amounts to be credited to the subaccount in the fiscal year in which the report is submitted.

(C) The estimated amounts of outlays to be paid out of the subaccount in the fiscal year in which the report is submitted.

(D) The estimated balance of the subaccount at the end of the fiscal year in which the report is submitted.

(E) A statement of how much of the estimated balance at the end of the fiscal year in which the report is submitted will be needed to pay outlays in the immediately following fiscal year that are in excess of the amount to be credited to the subaccount in the immediately following fiscal year.

(r) NOTIFICATION OF TRANSFERS.—(1) Notwithstanding any authority provided in this section to transfer funds, the transfer of funds from a working-capital fund, including a transfer to another working-capital fund, shall not be made under such authority unless the Secretary of Defense submits, in advance, a notification of the proposed transfer to the congressional defense committees in accordance with customary procedures.

(2) The amount of a transfer covered by a notification under paragraph (1) that is made in a fiscal year does not count toward any limitation on the total amount of transfers that may be made for that fiscal year under authority provided to the Secretary of Defense in a law authorizing appropriations for a fiscal year for military activities of the Department of Defense or a law making appropriations for the Department of Defense.

(s) LIMITATION ON CESSATION OR SUSPENSION OF DISTRIBUTION OF FUNDS FOR CERTAIN WORKLOAD.—(1) Except as provided in paragraph (2), the Secretary of Defense or the Secretary of a military department is not authorized—

(A) to suspend the employment of indirectly funded Government employees of the Department of Defense who are paid for out of working-capital funds by ceasing or suspending the distribution of such funds; or

(B) to cease or suspend the distribution of funds from a working-capital fund for a current project undertaken to carry out the functions or activities of the Department.

(2) Paragraph (1) shall not apply with respect to a working-capital fund if—

(A) the working-capital fund is insolvent; or

(B) there are insufficient funds in the working-capital fund to pay labor costs for the current project concerned.

(3) The Secretary of Defense or the Secretary of a military department may waive the limitation in paragraph (1) if such Secretary determines that the waiver is in the national security interests of the United States.

(4) This subsection shall not be construed to provide for the exclusion of any particular category of employees of the Department of Defense from furlough due to absence of or inadequate funding.

(t) MARKET FLUCTUATION ACCOUNT.—(1) From amounts available for Working Capital Fund, Defense, the Secretary shall reserve up to $1,000,000,000, to remain available without fiscal year limitation, for petroleum market price fluctuations. Such amounts may only be disbursed if the Secretary determines such a disbursement is necessary to absorb volatile market changes in fuel prices without affecting the standard price charged for fuel.

(2) A budget request for the anticipated costs of fuel may not take into account the availability of funds reserved under paragraph (1).

(u) USE FOR UNSPECIFIED MINOR MILITARY CONSTRUCTION PROJECTS TO REVITALIZE AND RECAPITALIZE DEFENSE INDUSTRIAL BASE FACILITIES.—(1) The Secretary of a military department may use a working capital fund of the department under this section to fund an unspecified minor military construction project under section 2805 of this title for the revitalization and recapitalization of a defense industrial base facility owned by the United States and under the jurisdiction of the Secretary.

(2)(A) Except as provided in subparagraph (B), section 2805 of this title shall apply with respect to a project funded using a working capital fund under the authority of this subsection in the same manner as such section applies to any unspecified minor military construction project under section 2805 of this title.

(B) For purposes of applying subparagraph (A), the dollar limitation specified in subsection (a)(2) of section 2805 of this title, subject to adjustment as provided in subsection (f) of such section, shall apply rather than the dollar limitation specified in subsection (c) of such section.

(3) In this subsection, the term ''defense industrial base facility'' means any Department of Defense depot, arsenal, shipyard, or plant located within the United States.

(4) The authority to use a working capital fund to fund a project under the authority of this subsection expires on September 30, 2025.

(Added Pub. L. 87–651, title II, §207(a), Sept. 7, 1962, 76 Stat. 521; amended Pub. L. 97–295, §1(22), Oct. 12, 1982, 96 Stat. 1290; Pub. L. 98–94, title XII, §1204(a), Sept. 24, 1983, 97 Stat. 683; Pub. L. 98–525, title III, §305, Oct. 19, 1984, 98 Stat. 2513; Pub. L. 100–26, §7(d)(2), Apr. 21, 1987, 101 Stat. 280; Pub. L. 101–510, div. A, title VIII, §801, title XIII, §1301(6), Nov. 5, 1990, 104 Stat. 1588, 1668; Pub. L. 102–172, title VIII, §8137, Nov. 26, 1991, 105 Stat. 1212; Pub. L. 102–484, div. A, title III, §374, Oct. 23, 1992, 106 Stat. 2385; Pub. L. 103–160, div. A, title I, §158(b), Nov. 30, 1993, 107 Stat. 1582; Pub. L. 105–85, div. A, title X, §1011(a), (b), Nov. 18, 1997, 111 Stat. 1873; Pub. L. 105–261, div. A, title X, §§1007(e)(1), 1008(a), Oct. 17, 1998, 112 Stat. 2115; Pub. L. 105–262, title VIII, §8146(d)(1), Oct. 17, 1998, 112 Stat. 2340; Pub. L. 106–65, div. A, title III, §§331(a)(1), 332, title X, §1066(a)(16), Oct. 5, 1999, 113 Stat. 566, 567, 771; Pub. L. 106–398, §1 [[div. A], title III, §341(f)], Oct. 30, 2000, 114 Stat. 1654, 1654A–64; Pub. L. 108–375, div. A, title X, §1009, Oct. 28, 2004, 118 Stat. 2037; Pub. L. 111–383, div. A, title XIV, §1403, Jan. 7, 2011, 124 Stat. 4410; Pub. L. 112–81, div. B, title XXVIII, §2802(c)(1), Dec. 31, 2011, 125 Stat. 1684; Pub. L. 114–92, div. A, title XIV, §§1421, 1422, Nov. 25, 2015, 129 Stat. 1083, 1084; Pub. L. 115–91, div. A, title II, §212, Dec. 12, 2017, 131 Stat. 1324; Pub. L. 115–232, div. A, title III, §321, title VIII, §809(a), title XIV, §1422, Aug. 13, 2018, 132 Stat. 1718, 1840, 2093; Pub. L. 116–92, div. A, title III, §352, title XVII, §1731(a)(29), Dec. 20, 2019, 133 Stat. 1320, 1813; Pub. L. 116–283, div. A, title III, §366, Jan. 1, 2021, 134 Stat. 3551; Pub. L. 117–263, div. A, title III, §§354, 372, Dec. 23, 2022, 136 Stat. 2534, 2540.)

HISTORICAL AND REVISION NOTES

1956 ACT

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2208(a)	5:172d(a).	July 26, 1947, ch. 343, §405; added Aug. 10, 1949, ch. 412, §11 (8th through 15th pars.), 63 Stat. 587.
2208(b)	5:172d(b).	
2208(c)	5:172d(c) (less 2d sentence).	
2208(d)	5:172d(d).	
2208(e)	5:172d(e)	
2208(f)	5:172d(f).	
2208(g)	5:172d(h).	
2208(h)	5:172d(g).	
2208(i)	5:172d(c) (2d sentence).	

In subsection (a)(1), (c)(1), (f), (g), and (h), the words ''stores, . . . materials, and equipment'' are omitted as covered by the word ''supplies'', as defined in section 101(26) of title 10.

In subsection (c), the word ''used'' is substituted for the word ''consumed''. The words ''and costs of using equipment'' are inserted to reflect an opinion of the Assistant General Counsel (Fiscal Matters), Department of Defense, February 2, 1960.

In subsection (d), the first sentence (less 1st 18 words) of 5 U.S.C. 172d(d) is omitted as executed.

In subsection (h), the following substitutions are made: ''prescribe'' for ''issue''; and ''persons'' for ''purchasers or users''. The word ''shall'' is substituted for the words ''is authorized to'' in the first sentence and for the word ''may'' in the last sentence to reflect the opinion of the Assistant General Counsel (Fiscal Matters), October 2, 1959, that the source law requires the action in question.

1982 ACT

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2208(h) (3d sentence).	10:2208 (note).	Dec. 21, 1979, Pub. L. 96–154, §767, 93 Stat. 1163.

The word ''hereafter'' is omitted as executed.

Editorial Notes

REFERENCES IN TEXT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, referred to in subsec. (*l*)(3)(B), is Pub. L. 93–288, May 22, 1974, 88 Stat. 143, which is classified principally to chapter 68 (§5121 et seq.) 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 5121 of Title 42 and Tables.

PRIOR PROVISIONS

Provisions similar to those in subsecs. (m) to (q) of this section were contained in section 2216a of this title prior to repeal by Pub. L. 105–261, §1008(b).

AMENDMENTS

2022—Subsec. (*l*)(3). Pub. L. 117–263, §354, designated existing provisions as subpar. (A), substituted ''Except as provided in subparagraph (B), the total'' for ''The total'', and added subpar. (B).

Subsec. (u)(4). Pub. L. 117–263, §372, substituted ''2025'' for ''2023''.

2021—Subsec. (*l*)(4), (5). Pub. L. 116–283 added par. (4) and redesignated former par. (4) as (5).

2019—Subsec. (u). Pub. L. 116–92, §1731(a)(29), inserted ''of this title'' after ''2805'' wherever appearing.

Subsec. (u)(1). Pub. L. 116–92, §352(1), substituted ''to fund'' for ''to carry out''.

Subsec. (u)(2). Pub. L. 116–92, §352(2), designated existing provisions as subpar. (A), substituted ''Except as provided in subparagraph (B), section 2805'' for ''Section 2805'' and ''carried out with'' for ''funded using'', and added subpar. (B).

Subsec. (u)(4). Pub. L. 116–92, §352(3), substituted ''to fund'' for ''to carry out''.

2018—Subsec. (e). Pub. L. 115–232, §1422, inserted at end ''The accomplishment of the most economical and efficient organization and operation of working capital fund activities for the purposes of this subsection shall include actions toward the following:

''(1) Undertaking efforts to optimize the rate structure for all requisitioning entities.

''(2) Encouraging a working capital fund activity to perform reimbursable work for other entities to sustain the efficient use of the workforce.

''(3) Determining the appropriate leadership level for approving work from outside entities to maximize efficiency.''

Subsec. (i). Pub. L. 115–232, §809(a), substituted ''section 7543'' for ''section 4543''.

Subsec. (u). Pub. L. 115–232, §321, added subsec. (u).

2017—Subsec. (k)(2). Pub. L. 115–91 substituted ''$500,000 for procurements by a major range and test facility installation or a science and technology reinvention laboratory and not less than $250,000 for procurements at all other facilities'' for ''$250,000'' in introductory provisions.

2015—Subsec. (s). Pub. L. 114–92, §1421, added subsec. (s).

Subsec. (t). Pub. L. 114–92, §1422, added subsec. (t).

2011—Subsec. (c)(1). Pub. L. 111–383, §1403(1), inserted before semicolon '', including the cost of the procurement and qualification of technology-enhanced maintenance capabilities that improve either reliability, maintainability, sustainability, or supportability and have, at a minimum, been demonstrated to be functional in an actual system application or operational environment''.

Subsec. (k)(2). Pub. L. 111–383, §1403(2), substituted ''$250,000'' for ''$100,000'' in introductory provisions.

Subsec. (k)(2)(A). Pub. L. 112–81, §2802(c)(1)(A), substituted ''section 2805(c)'' for ''section 2805(c)(1)''.

Subsec. (*o*)(2)(A). Pub. L. 112–81, §2802(c)(1)(B), substituted ''section 2805(c)'' for ''section 2805(c)(1)''.

2004—Subsec. (r). Pub. L. 108–375 added subsec. (r).

2000—Subsec. (j)(1). Pub. L. 106–398 substituted ''contract, and the solicitation'' for ''contract; and'' at end of subpar. (A) and all that follows through ''(B) the solicitation'', substituted ''; or'' for period after ''private firms'', and added a new subpar. (B).

1999—Subsec. (j). Pub. L. 106–65, §§331(a)(1), 332, designated existing provisions as par. (1), redesignated former pars. (1) and (2) as subpars. (A) and (B), respectively, substituted '', remanufacturing, and engineering'' for ''or remanufacturing'' in introductory provisions, inserted ''or a subcontract under a Department of Defense contract'' before the semicolon in subpar. (A), substituted ''solicitation for the contract or subcontract'' for ''Department of Defense solicitation for such contract'' in subpar. (B), and added par. (2).

Subsec. (*l*)(2)(A). Pub. L. 106–65, §1066(a)(16), inserted ''of'' after ''during a period''.

1998—Subsec. (*l*)(3), (4). Pub. L. 105–261, §1007(e)(1), and Pub. L. 105–262 amended subsec. (*l*) identically, adding par. (3) and redesignating former par. (3) as (4).

Subsecs. (m) to (q). Pub. L. 105–261, §1008(a), added subsecs. (m) to (q).

1997—Subsec. (k). Pub. L. 105–85, §1011(a), added subsec. (k) and struck out former subsec. (k) which read as follows: ''The Secretary of Defense shall provide that of the total amount of payments received in a fiscal year by funds established under this section for industrial-type activities, not less than 3 percent during fiscal year 1985, not less than 4 percent during fiscal year 1986, and not less than 5 percent during fiscal year 1987 shall be used for the acquisition of capital equipment for such activities.''

Subsec. (*l*). Pub. L. 105–85, §1011(b), added subsec. (*l*).

1993—Subsec. (i). Pub. L. 103–160 amended subsec. (i) generally. Prior to amendment, subsec. (i) required that regulations under subsec. (h) authorize working-capital funded Army industrial facilities to sell manufactured articles and services to persons outside the Department of Defense in specified cases.

1992—Subsec. (j). Pub. L. 102–484 substituted ''The Secretary of a military department may authorize a working capital funded industrial facility of that department'' for ''The Secretary of the Army may authorize a working capital funded Army industrial facility''.

1991—Subsecs. (j), (k). Pub. L. 102–172 added subsec. (j) and redesignated former subsec. (j) as (k).

1990—Subsec. (i)(1). Pub. L. 101–510, §801, added par. (1), redesignated par. (3) as (2), and struck out former pars. (1) and (2) which read as follows:

''(1) Regulations under subsection (h) may authorize an article manufactured by a working-capital funded Department of the Army arsenal that manufactures large caliber cannons, gun mounts, or recoil mechanisms to be sold to a person outside the Department of Defense if—

''(A) the article is sold to a United States manufacturer, assembler, or developer (i) for use in developing new products, or (ii) for incorporation into items to be sold to, or to be used in a contract with, an agency of the United States or a friendly foreign government;

''(B) the purchaser is determined by the Department of Defense to be qualified to carry out the proposed work involving the article to be purchased;

''(C) the article is not readily available from a commercial source in the United States; and

''(D) the sale is to be made on a basis that does not interfere with performance of work by the arsenal for the Department of Defense or for a contractor of the Department of Defense.

''(2) Services related to an article sold under this subsection may also be sold to the purchaser if the services are to be performed in the United States for the purchaser.''

Subsec. (k). Pub. L. 101–510, §1301(6), struck out subsec. (k) which read as follows: ''Reports annually shall be made to the President and to Congress on the condition and operation of working-capital funds established under this section.''

1987—Subsec. (i)(3). Pub. L. 100–26 inserted ''(22 U.S.C. 2778)'' after ''Arms Export Control Act''.

1984—Subsecs. (i) to (k). Pub. L. 98–525 added subsecs. (i) and (j) and redesignated former subsec. (i) as (k).

1983—Subsec. (d). Pub. L. 98–94 substituted ''In addition, such amounts may be appropriated for the purpose of providing capital for working-capital funds as have been specifically authorized by law'' for ''If this method does not, in the determination of the Secretary of Defense, provide adequate amounts of working capital, such amounts as may be necessary may be appropriated for that purpose''.

1982—Subsec. (h). Pub. L. 97–295 inserted provision that supplies available in inventories financed by working capital funds established under this section may be sold to contractors for use in performing contracts with the Department of Defense.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2018 AMENDMENT

Amendment by section 809(a) of Pub. L. 115–232 effective Feb. 1, 2019, with provision for the coordination of amendments and special rule for certain redesigna-

tions, see section 800 of Pub. L. 115–232, set out as a note preceding section 3001 of this title.

EFFECTIVE DATE OF 1998 AMENDMENT

Pub. L. 105–261, div. A, title X, §1007(e)(2), Oct. 17, 1998, 112 Stat. 2115, and Pub. L. 105–262, title VIII, §8146(d)(2), Oct. 17, 1998, 112 Stat. 2340, provided that: ''Section 2208(*l*)(3) of such title, as added by paragraph (1), applies to fiscal years after fiscal year 1999.''

EFFECTIVE DATE OF 1983 AMENDMENT

Pub. L. 98–94, title XII, §1204(b), Sept. 24, 1983, 97 Stat. 683, provided that: ''The amendment made by subsection (a) [amending this section] shall apply only with respect to appropriations for fiscal years beginning after September 30, 1984.''

ADVANCE BILLING FOR FISCAL YEAR 2022

Pub. L. 117–103, div. C, title VIII, §8117, Mar. 15, 2022, 136 Stat. 203, provided that: ''During fiscal year 2022, the monetary limitation imposed by section 2208(*l*)(3) of title 10, United States Code[,] may be exceeded by up to $1,000,000,000.''

ADVANCE BILLING FOR FISCAL YEAR 2020

Pub. L. 116–136, div. B, title III, §13003, Mar. 27, 2020, 134 Stat. 522, provided that:

''(a) Notwithstanding section 2208(*l*)(3) of title 10, United States Code, during fiscal year 2020, the total amount of the advance billings rendered or imposed for all working-capital funds of the Department of Defense may exceed the amount otherwise specified in such section.

''(b) In this section, the term 'advance billing' has the meaning given that term in section 2208(*l*)(4) [now 2208(*l*)(5)] of title 10, United States Code.''

PILOT PROGRAM FOR ACQUISITION OF COMMERCIAL SATELLITE COMMUNICATION SERVICES

Pub. L. 113–291, div. A, title XVI, §1605, Dec. 19, 2014, 128 Stat. 3623, as amended by Pub. L. 114–92, div. A, title XVI, §1612, Nov. 25, 2015, 129 Stat. 1103; Pub. L. 114–328, div. A, title XVI, §1606(a), Dec. 23, 2016, 130 Stat. 2586, provided that:

''(a) PILOT PROGRAM.—

''(1) IN GENERAL.—The Secretary of Defense shall develop and carry out a pilot program to effectively and efficiently acquire commercial satellite communications services to meet the requirements of the military departments, Defense Agencies, and combatant commanders.

''(2) FUNDING.—Of the funds authorized to be appropriated for any of fiscal years 2015 through 2020 for the Department of Defense for the acquisition of satellite communications, not more than $50,000,000 may be obligated or expended for such pilot program during such a fiscal year.

''(3) CERTAIN AUTHORITIES.—In carrying out the pilot program under paragraph (1), the Secretary may not use the authorities provided in sections 2208(k) and 2210(b) of title 10, United States Code.

''(4) METHODS.—In carrying out the pilot program under paragraph (1), the Secretary may use a variety of methods authorized by law to effectively and efficiently acquire commercial satellite communications services, including by carrying out multiple pathfinder activities under the pilot program.

''(b) GOALS.—In developing and carrying out the pilot program under subsection (a)(1), the Secretary shall ensure that the pilot program—

''(1) provides a cost-effective and strategic method to acquire commercial satellite communications services;

''(2) incentivizes private-sector participation and investment in technologies to meet future requirements of the Department of Defense with respect to commercial satellite communications services;

''(3) takes into account the potential for a surge or other change in the demand of the Department for commercial satellite communications services in response to global or regional events;

''(4) ensures the ability of the Secretary to control and account for the cost of programs and work performed under the pilot program; and

''(5) demonstrates the potential to achieve order-of-magnitude improvements in satellite communications capability.

''(c) DURATION.—The pilot program under subsection (a)(1) shall terminate on October 1, 2020.

''(d) REPORTS AND BRIEFINGS.—

''(1) INITIAL REPORT.—Not later than 270 days after the date of the enactment of this Act [Dec. 19, 2014], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that includes—

''(A) a plan and schedule to carry out the pilot program under subsection (a)(1); and

''(B) a description of the appropriate metrics established by the Secretary to meet the goals of the pilot program.

''(2) BRIEFING.—At the same time as the President submits to Congress the budget pursuant to section 1105 of title 31, for each of fiscal years 2017 through 2020, the Secretary shall provide to the congressional defense committees briefing on the pilot program.

''(3) FINAL REPORT.—Not later than December 1, 2020, the Secretary shall submit to the congressional defense committees a report on the pilot program under subsection (a)(1). The report shall include—

''(A) an assessment of the pilot program and whether the pilot program effectively and efficiently acquires commercial satellite communications services to meet the requirements of the military departments, Defense Agencies, and combatant commanders; and

''(B) a description of—

''(i) any contract entered into under the pilot program, the funding used under such contract, and the efficiencies realized under such contract;

''(ii) the advantages and challenges of using the pilot program;

''(iii) any additional authorities the Secretary determines necessary to acquire commercial satellite communications services as described in subsection (a)(1); and

''(iv) any recommendations of the Secretary with respect to improving or extending the pilot program.

''(e) IMPLEMENTATION OF GOALS.—In developing and carrying out the pilot program under subsection (a)(1), by not later than September 30, 2017, the Secretary shall take actions to begin the implementation of each goal specified in subsection (b).''

ADVANCE BILLING FOR FISCAL YEAR 2006

Pub. L. 109–234, title I, §1206, June 15, 2006, 120 Stat. 430, provided in part that: ''Notwithstanding 10 U.S.C. 2208(*l*), the total amount of advance billings rendered or imposed for all working capital funds of the Department of Defense in fiscal year 2006 shall not exceed $1,200,000,000''.

ADVANCE BILLING FOR FISCAL YEAR 2005

Pub. L. 109–13, div. A, title I, §1005, May 11, 2005, 119 Stat. 243, provided that for fiscal year 2005, the limitation under subsec. (*l*)(3) of this section on the total amount of advance billings rendered or imposed for all working capital funds of the Department of Defense in a fiscal year would be applied by substituting ''$1,500,000,000'' for ''$1,000,000,000''.

OVERSIGHT OF DEFENSE BUSINESS OPERATIONS FUND

Pub. L. 103–337, div. A, title III, §311(b)–(e), Oct. 5, 1994, 108 Stat. 2708, which related to purchase from other sources, limitation on inclusion of certain costs in DBOF charges, procedures for accumulation of funds, and annual reports and budget, was repealed and re-

stated in section 2216a(d)(2)(B), (f) to (h)(3) of this title by Pub. L. 104–106, div. A, title III, §371(a)(1), (b)(1), Feb. 10, 1996, 110 Stat. 277–279.

Pub. L. 103–337, div. A, title III, §311(f), (g), Oct. 5, 1994, 108 Stat. 2709, required Secretary of Defense to submit to congressional defense committees, not later than Feb. 1, 1995, a report on progress made in implementing the Defense Business Operations Fund Improvement Plan, dated September 1993, and required Comptroller General to monitor and evaluate the Department of Defense implementation of the Plan and to report to congressional defense committees not later than Mar. 1, 1995.

CHARGES FOR GOODS AND SERVICES PROVIDED THROUGH DEFENSE BUSINESS OPERATIONS FUND

Pub. L. 103–160, div. A, title III, §333(a), (b), Nov. 30, 1993, 107 Stat. 1621, which provided that charges for goods and services provided through Defense Business Operations Fund were to include amounts necessary to recover full costs of development, implementation, operation, and maintenance of systems supporting wholesale supply and maintenance activities of Department of Defense and use of military personnel in provision of goods and services, and were not to include amounts necessary to recover costs of military construction project other than minor construction project financed by Defense Business Operations Fund pursuant to section 2805(c)(1) of this title, and which required full cost of operation of Defense Finance Accounting Service to be financed within Defense Business Operations Fund through charges for goods and services provided through Fund, was repealed and restated in section 2216a(d)(1)(A), (C), (2)(A) of this title by Pub. L. 104–106, div. A, title III, §371(a)(1), (b)(2), Feb. 10, 1996, 110 Stat. 277–279.

CAPITAL ASSET SUBACCOUNT

Pub. L. 102–484, div. A, title III, §342, Oct. 23, 1992, 106 Stat. 2376, as amended by Pub. L. 103–160, div. A, title III, §333(c), Nov. 30, 1993, 107 Stat. 1622, which provided that charges for goods and services provided through the Defense Business Operations Fund include amounts for depreciation of capital assets which were to be credited to a separate capital asset subaccount in the Fund, authorized Secretary of Defense to award contracts for capital assets of the Fund in advance of availability of funds in the subaccount, required Secretary to submit annual reports to congressional defense committees, authorized appropriations to the Fund for fiscal years 1993 and 1994, and defined terms, was repealed and restated in section 2216a(d)(1)(B), (e), (h)(4), and (i) of this title by Pub. L. 104–106, div. A, title III, §371(a)(1), (b)(3), Feb. 10, 1996, 110 Stat. 277–279.

LIMITATIONS ON USE OF DEFENSE BUSINESS OPERATIONS FUND

Pub. L. 102–190, div. A, title III, §316, Dec. 5, 1991, 105 Stat. 1338, as amended by Pub. L. 102–484, div. A, title III, §341, Oct. 23, 1992, 106 Stat. 2374; Pub. L. 103–160, div. A, title III, §§331, 332, Nov. 30, 1993, 107 Stat. 1620; Pub. L. 103–337, div. A, title III, §311(a), Oct. 5, 1994, 108 Stat. 2708, which authorized Secretary of Defense to manage performance of certain working-capital funds established under this section, the Defense Finance and Accounting Service, the Defense Industrial Plan Equipment Center, the Defense Commissary Agency, the Defense Technical Information Service, the Defense Reutilization and Marketing Service, and certain activities funded through use of working-capital fund established under this section, directed Secretary to maintain separate accounting, reporting, and auditing of such funds and activities, required Secretary to submit to congressional defense committees, by not later than 30 days after Nov. 30, 1993, a comprehensive management plan and, by not later than Feb. 1, 1994, a progress report on plan's implementation, and directed Comptroller General to monitor and evaluate the plan and submit to congressional defense committees, not later than Mar. 1, 1994, a report, was repealed and restated in section 2216a(a)–(c) of this title by Pub. L. 104–106, div. A, title III, §371(a)(1), (b)(4), Feb. 10, 1996, 110 Stat. 277, 279.

DEFENSE BUSINESS OPERATIONS FUND

Pub. L. 102–172, title VIII, §8121, Nov. 26, 1991, 105 Stat. 1204, which established on the books of the Treasury a fund entitled the ''Defense Business Operations Fund'' to be operated as a working capital fund under the provisions of this section and to include certain existing organizations including the Defense Finance and Accounting Service, the Defense Commissary Agency, the Defense Technical Information Center, the Defense Reutilization and Marketing Service, and the Defense Industrial Plant Equipment Service, directed transfer of assets and balances of those organizations to the Fund, provided for budgeting and accounting of charges for supplies and services provided by the Fund, and directed that capital asset charges collected be credited to a subaccount of the Fund, was repealed by Pub. L. 104–106, div. A, title III, §371(b)(5), Feb. 10, 1996, 110 Stat. 280.

SALE OF INVENTORIES FOR PERFORMANCE OF CONTRACTS WITH DEFENSE DEPARTMENT

Pub. L. 96–154, title VII, §767, Dec. 21, 1979, 93 Stat. 1163, which had provided that supplies available in inventories financed by working capital funds established pursuant to this section could, on and after Dec. 21, 1979, be sold to contractors for use in performing contracts with the Department of Defense, was repealed and restated in subsec. (h) of this section by Pub. L. 97–295, §§1(22), 6(b), Oct. 12, 1982, 96 Stat. 1290, 1315.

§ 2209. Management funds

(a) To conduct economically and efficiently the operations of the Department of Defense that are financed by at least two appropriations but whose costs cannot be immediately distributed and charged to those appropriations, there is the Army Management Fund, the Navy Management Fund, and the Air Force Management Fund, each within its respective department and under the direction of the Secretary of that department. Each such fund shall consist of a corpus of $1,000,000 and such amounts as may be appropriated thereto from time to time. An account for an operation that is to be financed by such a fund may be established only with the approval of the Secretary of Defense.

(b) Under such regulations as the Secretary of Defense may prescribe, expenditures may be made from a management fund for material (other than for stock), personal services, and services under contract. However, obligation may not be incurred against that fund if it is not chargeable to funds available under an appropriation of the department concerned or funds of another department or agency of the Department of Defense. The fund shall be promptly reimbursed from those funds for expenditures made from it.

(c) Notwithstanding any other provision of law, advances, by check or warrant, or reimbursements, may be made from available appropriations to a management fund on the basis of the estimated cost of a project. As adequate data becomes available, the estimated cost shall be revised and necessary adjustments made. Final adjustment shall be made with the appropriate funds for the fiscal year in which the advances or reimbursements are made. Except as otherwise provided by law, amounts advanced to

management funds are available for obligation only during the fiscal year in which they are advanced.

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 522.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2209(a)	5:172e(a), (b).	July 3, 1942, ch. 484; restated Aug. 10, 1949, ch. 412, § 11 (16th through 19th pars.), 63 Stat. 588.
2209(b)	5:172e(c) (last sentence).	
2209(c)	5:172e(c) (less last sentence).	
	5:172e(d).	

In subsection (a), the second sentence is substituted for the second sentence of 5 U.S.C. 172e(a) and the first sentence (less last 21 words) of 5 U.S.C. 172e(b) which are omitted as unnecessary.

In subsection (c), the 13th through 33d words of 5 U.S.C. 172e(d) are omitted as surplusage.

§ 2210. Proceeds of sales of supplies: credit to appropriations

(a)(1) A working-capital fund established pursuant to section 2208 of this title may retain so much of the proceeds of disposals of property referred to in paragraph (2) as is necessary to recover the expenses incurred by the fund in disposing of such property. Proceeds from the sale or disposal of such property in excess of amounts necessary to recover the expenses may be credited to current applicable appropriations of the Department of Defense.

(2) Paragraph (1) applies to disposals of supplies, material, equipment, and other personal property that were not financed by stock funds established under section 2208 of this title.

(b) Obligations may, without regard to fiscal year limitations, be incurred against anticipated reimbursements to stock funds in such amounts and for such period as the Secretary of Defense, with the approval of the President, may determine to be necessary to maintain stock levels consistently with planned operations for the next fiscal year.

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 522; amended Pub. L. 96–513, title V, § 511(72), Dec. 12, 1980, 94 Stat. 2926; Pub. L. 105–261, div. A, title X, § 1009, Oct. 17, 1998, 112 Stat. 2117.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2210(a)	5:172d–1 (less proviso).	Aug. 1, 1953, ch. 305, § 645, 67 Stat. 357.
2210(b)	5:172d–1 (proviso).	

In section (a), the words ''proceeds of the disposal'' are substituted for the words ''moneys arising from the disposition''.

Editorial Notes

AMENDMENTS

1998—Subsec. (a). Pub. L. 105–261 amended subsec. (a) generally. Prior to amendment, subsec. (a) read as follows: ''Current applicable appropriations of the Department of Defense may be credited with proceeds of the disposals of supplies that are not financed by stock funds established under section 2208 of this title.''

1980—Subsec. (b). Pub. L. 96–513 substituted ''President'' for ''Director of the Bureau of the Budget''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 1980 AMENDMENT

Amendment by Pub. L. 96–513 effective Dec. 12, 1980, see section 701(b)(3) of Pub. L. 96–513, set out as a note under section 101 of this title.

§ 2211. Reimbursement for equipment, material, or services furnished members of the United Nations

Amounts paid by members of the United Nations for equipment or materials furnished, or services performed, in joint military operations shall be credited to appropriate appropriations of the Department of Defense in the manner authorized by section 632(d) of the Foreign Assistance Act of 1961 (22 U.S.C. 2392(d)).

(Added Pub. L. 87–651, title II, § 207(a), Sept. 7, 1962, 76 Stat. 522; amended Pub. L. 96–513, title V, § 511(73), Dec. 12, 1980, 94 Stat. 2926.)

HISTORICAL AND REVISION NOTES

Revised section	*Source (U.S. Code)*	*Source (Statutes at Large)*
2211	5:171m–1.	Jan. 6, 1951, ch. 1213, § 703, 64 Stat. 1235.

The reference to section 2392(d) of title 22 is substituted for the reference to section 1574(b) of that title to reflect section 542(b) of the Act of August 26, 1954, ch. 937 (68 Stat. 861) and section 642(a)(2) and (b) of the Act of September 4, 1961, Pub. L. 87–195 (75 Stat. 460).

Editorial Notes

AMENDMENTS

1980—Pub. L. 96–513 substituted ''section 632(d) of the Foreign Assistance Act of 1961 (22 U.S.C. 2392(d))'' for ''section 2392(d) of title 22''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 1980 AMENDMENT

Amendment by Pub. L. 96–513 effective Dec. 12, 1980, see section 701(b)(3) of Pub. L. 96–513, set out as a note under section 101 of this title.

[§ 2212. Renumbered § 3138]

Editorial Notes

PRIOR PROVISIONS

A prior section 2212, added Pub. L. 100–370, § 1(d)(2)(A), July 19, 1988, 102 Stat. 842, directed Secretary of Defense to maintain within each military department an accounting procedure to aid in identification and control of expenditures for contracted advisory and assistance services, prior to repeal by Pub. L. 103–355, title II, § 2454(c)(1), Oct. 13, 1994, 108 Stat. 3326.

Another prior section 2212, added Pub. L. 95–356, title VIII, § 802(a)(1), Sept. 8, 1978, 92 Stat. 585; amended Pub. L. 97–258, § 3(b)(5), Sept. 18, 1982, 96 Stat. 1063, related to transmission of annual military construction authorization request, prior to repeal by Pub. L. 97–214, § 7(1), July 12, 1982, 96 Stat. 173, eff. Oct. 1, 1982, applicable to military construction projects, and to construction and acquisition of military family housing authorized before, on, or after such date. See section 2859 of this title.

[§ 2213. Renumbered § 3070]

Editorial Notes

PRIOR PROVISIONS

A prior section 2213 was renumbered section 2350c of this title.

§ 2214. Transfer of funds: procedure and limitations

(a) PROCEDURE FOR TRANSFER OF FUNDS.—Whenever authority is provided in an appropriation Act to transfer amounts in working capital funds or to transfer amounts provided in appropriation Acts for military functions of the Department of Defense (other than military construction) between such funds or appropriations (or any subdivision thereof), amounts transferred under such authority shall be merged with and be available for the same purposes and for the same time period as the fund or appropriations to which transferred.

(b) LIMITATIONS ON PROGRAMS FOR WHICH AUTHORITY MAY BE USED.—Such authority to transfer amounts—

(1) may not be used except to provide funds for a higher priority item, based on unforeseen military requirements, than the items for which the funds were originally appropriated; and

(2) may not be used if the item to which the funds would be transferred is an item for which Congress has denied funds.

(c) NOTICE TO CONGRESS.—The Secretary of Defense shall promptly notify the Congress of each transfer made under such authority to transfer amounts.

(d) LIMITATIONS ON REQUESTS TO CONGRESS FOR REPROGRAMMINGS.—Neither the Secretary of Defense nor the Secretary of a military department may prepare or present to the Congress, or to any committee of either House of the Congress, a request with respect to a reprogramming of funds—

(1) unless the funds to be transferred are to be used for a higher priority item, based on unforeseen military requirements, than the item for which the funds were originally appropriated; or

(2) if the request would be for authority to reprogram amounts to an item for which the Congress has denied funds.

(Added Pub. L. 101–510, div. A, title XIV, § 1482(c)(1), Nov. 5, 1990, 104 Stat. 1709.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Oct. 1, 1991, see section 1482(d) of Pub. L. 101–510, set out as an Effective Date of 1990 Amendment note under section 119 of this title.

NOTIFICATION TO CONGRESS OF REPROGRAMMING INVOLVING MILITARY CONSTRUCTION FUNDS

Pub. L. 118–159, div. B, title XXVIII, § 2810, Dec. 23, 2024, 138 Stat. 2252, provided that: ''The Secretary of Defense shall notify the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] of any reprogramming of funds made available for military construction not later than 14 days after the date of such reprogramming.''

§ 2215. Transfer of funds to other departments and agencies: limitation

Funds available for military functions of the Department of Defense may not be made available to any other department or agency of the Federal Government pursuant to a provision of law enacted after November 29, 1989, unless, not less than 30 days before such funds are made available to such other department or agency, the Secretary of Defense submits to the congressional defense committees a certification that making those funds available to such other department or agency is in the national security interest of the United States.

(Added Pub. L. 103–160, div. A, title XI, § 1106(a)(1), Nov. 30, 1993, 107 Stat. 1750; amended Pub. L. 104–106, div. A, title XV, § 1502(a)(14), Feb. 10, 1996, 110 Stat. 503; Pub. L. 106–65, div. A, title X, § 1067(1), Oct. 5, 1999, 113 Stat. 774; Pub. L. 108–375, div. A, title X, § 1084(b)(1), Oct. 28, 2004, 118 Stat. 2060.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2215, added Pub. L. 99–661, div. A, title XIII, § 1307(a)(1), Nov. 14, 1986, 100 Stat. 3980, related to reports on unobligated balances, prior to repeal by Pub. L. 101–510, div. A, title XIII, § 1301(7), Nov. 5, 1990, 104 Stat. 1668.

Provisions similar to those in this section were contained in Pub. L. 101–189, div. A, title XVI, § 1604, Nov. 29, 1989, 103 Stat. 1598, which was set out as a note under section 1531 of Title 31, Money and Finance, prior to repeal by Pub. L. 103–160, § 1106(b).

AMENDMENTS

2004—Pub. L. 108–375 struck out subsec. (a) designation and heading before ''Funds available'', substituted ''congressional defense committees'' for ''congressional committees specified in subsection (b)'', and struck out heading and text of subsec. (b). Text of subsec. (b) read as follows: ''The committees referred to in subsection (a) are—

''(1) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

''(2) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.''

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

1996—Pub. L. 104–106 designated existing provisions as subsec. (a), inserted heading, substituted ''to the congressional committees specified in subsection (b)'' for ''to the Committees on Armed Services and the Committees on Appropriations of the Senate and House of Representatives'', and added subsec. (b).

[§ 2216. Renumbered § 3136]

Editorial Notes

PRIOR PROVISIONS

A prior section 2216, added Pub. L. 104–106, div. A, title III, § 371(a)(1), Feb. 10, 1996, 110 Stat. 277, was renumbered section 2216a of this title and subsequently repealed.

Another prior section 2216, added Pub. L. 99–661, div. A, title XIII, § 1307(a)(1), Nov. 14, 1986, 100 Stat. 3980, related to annual reports on budgeting for inflation, prior to repeal by Pub. L. 101–510, div. A, title XIII, § 1301(8), Nov. 5, 1990, 104 Stat. 1668.

§ 2216a. Rapidly meeting urgent needs: Joint Urgent Operational Needs Fund

(a) ESTABLISHMENT.—There is established in the Treasury an account to be known as the ''Joint Urgent Operational Needs Fund'' (in this section referred to as the ''Fund'').

(b) ELEMENTS.—The Fund shall consist of the following:

(1) Amounts appropriated to the Fund.

(2) Amounts transferred to the Fund.

(3) Any other amounts made available to the Fund by law.

(c) USE OF FUNDS.—(1) Amounts in the Fund shall be available to the Secretary of Defense for capabilities that are determined by the Secretary, pursuant to the review process required by Department of Defense Instruction 5000.81 (or any successor instruction), dated December 31, 2019, and titled ''Urgent Capability Acquisition'', to be suitable for rapid fielding in response to urgent operational needs.

(2) The Secretary shall establish a merit-based process for identifying equipment, supplies, services, training, and facilities suitable for funding through the Fund.

(3) Nothing in this section shall be interpreted to require or enable any official of the Department of Defense to provide funding under this section pursuant to a congressional earmark, as defined in clause 9 of Rule XXI of the Rules of the House of Representatives, or a congressionally directed spending item, as defined in paragraph 5 of Rule XLIV of the Standing Rules of the Senate.

(d) TRANSFER AUTHORITY.—(1) Amounts in the Fund may be transferred by the Secretary of Defense from the Fund to any of the following accounts of the Department of Defense to accomplish the purpose stated in subsection (c):

(A) Operation and maintenance accounts.

(B) Procurement accounts.

(C) Research, development, test, and evaluation accounts.

(2) Upon determination by the Secretary that all or part of the amounts transferred from the Fund under paragraph (1) are not necessary for the purpose for which transferred, such amounts may be transferred back to the Fund.

(3) The transfer of an amount to an account under the authority in paragraph (1) shall be deemed to increase the amount authorized for such account by an amount equal to the amount so transferred.

(4) The transfer authority provided by paragraphs (1) and (2) is in addition to any other transfer authority available to the Department of Defense by law.

(e) SUNSET.—The authority to make expenditures or transfers from the Fund shall expire on September 30, 2018.

(Added Pub. L. 112–81, div. A, title VIII, §846(a)(1), Dec. 31, 2011, 125 Stat. 1516; amended Pub. L. 112–239, div. A, title X, §1076(e)(2), Jan. 2, 2013, 126 Stat. 1951; Pub. L. 113–291, div. A, title VIII, §860, Dec. 19, 2014, 128 Stat. 3461; Pub. L. 117–263, div. A, title VIII, §804(d)(1), Dec. 23, 2022, 136 Stat. 2701.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2216a, added Pub. L. 104–106, div. A, title III, §371(a)(1), Feb. 10, 1996, 110 Stat. 277, §2216; renumbered §2216a and amended Pub. L. 104–201, div. A, title III, §§363(c), 364, title X, §1074(a)(10), Sept. 23, 1996, 110 Stat. 2493, 2494, 2659, related to Defense Business Operations Fund, prior to repeal by Pub. L. 105–261, div. A, title X, §1008(b), Oct. 17, 1998, 112 Stat. 2117.

AMENDMENTS

2022—Subsec. (c)(1). Pub. L. 117–263 substituted ''Department of Defense Instruction 5000.81 (or any successor instruction), dated December 31, 2019, and titled 'Urgent Capability Acquisition''' for ''section 804(b) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (10 U.S.C. 2302 note)''.

2014—Subsec. (e). Pub. L. 113–291 substituted ''September 30, 2018'' for ''September 30, 2015''.

2013—Subsec. (e). Pub. L. 112–239 substituted ''on September 30, 2015.'' for ''on the last day of the third fiscal year that begins after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2012.''

Statutory Notes and Related Subsidiaries

LIMITATION ON COMMENCEMENT OF EXPENDITURES FROM FUND

Pub. L. 112–81, div. A, title VIII, §846(b), Dec. 31, 2011, 125 Stat. 1517, provided that: ''No expenditure may be made from the Joint Urgent Operational Needs Fund established by section 2216a of title 10, United States Code (as added by subsection (a)), until the Secretary of Defense certifies to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] that the Secretary has developed and implemented an expedited review process in compliance with the requirements of section 804 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4256; 10 U.S.C. 2302 note).''

[§ 2217. Renumbered § 3135]

§ 2218. National Defense Sealift Fund

(a) ESTABLISHMENT.—There is established in the Treasury of the United States a fund to be known as the ''National Defense Sealift Fund''.

(b) ADMINISTRATION OF FUND.—The Secretary of Defense shall administer the Fund consistent with the provisions of this section.

(c) FUND PURPOSES.—(1) Funds in the National Defense Sealift Fund shall be available for obligation and expenditure only for the following purposes:

(A) Construction (including design of vessels), purchase, alteration, and conversion of Department of Defense sealift vessels.

(B) Operation, maintenance, and lease or charter of Department of Defense vessels for national defense purposes.

(C) Installation and maintenance of defense features for national defense purposes on privately owned and operated vessels that are constructed in the United States and documented under the laws of the United States.

(D) Expenses for maintaining the National Defense Reserve Fleet under section 11 of the Merchant Ship Sales Act of 1946 (50 U.S.C. 4405),[1] and for the costs of acquisition of vessels for, and alteration and conversion of vessels in (or to be placed in), the fleet, but only for vessels built in United States shipyards.

(2) Funds in the National Defense Sealift Fund may be obligated or expended only in amounts authorized by law.

(3) Funds obligated and expended for a purpose set forth in subparagraph (B) of paragraph (1) may be derived only from funds deposited in the National Defense Sealift Fund pursuant to subsection (d)(1).

[1] See References in Text note below.

(d) DEPOSITS.—There shall be deposited in the Fund the following:

(1) All funds appropriated to the Department of Defense for—

(A) construction (including design of vessels), purchase, alteration, and conversion of national defense sealift vessels;

(B) operations, maintenance, and lease or charter of national defense sealift vessels; and

(C) installation and maintenance of defense features for national defense purposes on privately owned and operated vessels.

(2) All receipts from the disposition of national defense sealift vessels, excluding receipts from the sale, exchange, or scrapping of National Defense Reserve Fleet vessels under sections 57101–57104 and chapter 573 of title 46.

(3) All receipts from the charter of vessels under section 1424(c) of the National Defense Authorization Act for Fiscal Year 1991 (10 U.S.C. 8661 note).

(4) Any other funds made available to the Department of Defense to carry out any of the purposes described in subsection (c).

(e) ACCEPTANCE OF SUPPORT.—(1) The Secretary of Defense may accept from any person, foreign government, or international organization any contribution of money, personal property (excluding vessels), or assistance in kind for support of the sealift functions of the Department of Defense.

(2) Any contribution of property accepted under paragraph (1) may be retained and used by the Department of Defense or disposed of in accordance with procedures prescribed by the Secretary of Defense.

(3) The Secretary of Defense shall deposit in the Fund money and receipts from the disposition of any property accepted under paragraph (1).

(f) LIMITATIONS.—(1) A vessel built in a foreign ship yard may not be purchased with funds in the National Defense Sealift Fund pursuant to subsection (c)(1), unless specifically authorized by law.

(2) Construction, alteration, or conversion of vessels with funds in the National Defense Sealift Fund pursuant to subsection (c)(1) shall be conducted in United States ship yards and shall be subject to section 1424(b) of Public Law 101–510 (104 Stat. 1683).

(3)(A) Notwithstanding the limitations under subsection (c)(1)(D) and paragraph (1), the Secretary of Defense may, as part of a program to recapitalize the Ready Reserve Force component of the national defense reserve fleet and the Military Sealift Command surge fleet, purchase any used vessel, regardless of where such vessel was constructed if such vessel—

(i) participated in the Maritime Security Fleet; and

(ii) is available for purchase at a reasonable cost, as determined by the Secretary.

(B) If the Secretary determines that no used vessel meeting the requirements under clauses (i) and (ii) of subparagraph (A) is available, the Secretary may purchase a used vessel comparable to a vessel described in clause (i) of subparagraph (A), regardless of the source of the vessel or where the vessel was constructed, if such vessel is available for purchase at a reasonable cost, as determined by the Secretary.

(C) The Secretary may not use the authority under this paragraph to purchase more than 10 foreign constructed vessels.

(D) The Secretary shall ensure that the initial conversion, or modernization of any vessel purchased under the authority of subparagraph (A) occurs in a shipyard located in the United States.

(E) The Secretary may not use the authority under this paragraph to procure more than four foreign constructed vessels unless the Secretary submits to Congress, by not later than the second week of February of the fiscal year during which the Secretary plans to use such authority, a certification that—

(i) the Secretary has initiated an acquisition strategy for the construction in United States shipyards of not less than ten new vessels that are sealift vessels, auxiliary vessels, or a combination of such vessels; and

(ii) of such new vessels, the lead ship is anticipated to be delivered by not later than 2028.

(F) Not later than 30 days before the purchase of any vessel using the authority under this paragraph, the Secretary, in consultation with the Maritime Administrator, shall submit to the congressional defense committees a report that contains each of the following with respect to such purchase:

(i) The proposed date of the purchase.

(ii) The price at which the vessel would be purchased.

(iii) The anticipated cost of modernization of the vessel.

(iv) The proposed military utility of the vessel.

(v) The proposed date on which the vessel will be available for use by the Ready Reserve.

(vi) The contracting office responsible for the completion of the purchase.

(vii) Certification that—

(I) there was no vessel available for purchase at a reasonable price that was constructed in the United States; and

(II) the used vessel purchased supports the recapitalization of the Ready Reserve Force component of the National Defense Reserve Fleet or the Military Sealift Command surge fleet.

(viii) A detailed account of the criteria used to make the determination under subparagraph (B).

(G) The Secretary may not finalize or execute the final purchase of any vessel using the authority under this paragraph until 30 days after the date on which a report under subparagraph (F) is submitted with respect to such purchase.

(g) EXPIRATION OF FUNDS AFTER 5 YEARS.—No part of an appropriation that is deposited in the National Defense Sealift Fund pursuant to subsection (d)(1) shall remain available for obligation more than five years after the end of fiscal year for which appropriated except to the extent specifically provided by law.

(h) BUDGET REQUESTS.—Budget requests submitted to Congress for the National Defense Sealift Fund shall separately identify—

(1) the amount requested for programs, projects, and activities for construction (including design of vessels), purchase, alteration, and conversion of national defense sealift vessels;

(2) the amount requested for programs, projects, and activities for operation, maintenance, and lease or charter of national defense sealift vessels;

(3) the amount requested for programs, projects, and activities for installation and maintenance of defense features for national defense purposes on privately owned and operated vessels that are constructed in the United States and documented under the laws of the United States; and

(4) the amount requested for programs, projects, and activities for research and development relating to national defense sealift.

(i) TITLE OR MANAGEMENT OF VESSELS.—Nothing in this section (other than subsection (c)(1)(D)) shall be construed to affect or modify title to, management of, or funding responsibilities for, any vessel of the National Defense Reserve Fleet, or assigned to the Ready Reserve Force component of the National Defense Reserve Fleet, as established by section 57100 of title 46.

(j) CONTRACTS FOR INCORPORATION OF DEFENSE FEATURES IN COMMERCIAL VESSELS.—(1) The head of an agency may enter into a contract with a company submitting an offer for that company to install and maintain defense features for national defense purposes in one or more commercial vessels owned or controlled by that company in accordance with the purpose for which funds in the National Defense Sealift Fund are available under subsection (c)(1)(C). The head of the agency may enter into such a contract only after the head of the agency makes a determination of the economic soundness of the offer. As consideration for a contract with the head of an agency under this subsection, the company entering into the contract shall agree with the Secretary of Defense to make any vessel covered by the contract available to the Secretary, fully crewed and ready for sea, at any time at any port determined by the Secretary, and for whatever duration the Secretary determines necessary.

(2) The head of an agency may make advance payments to the contractor under a contract under paragraph (1) in a lump sum, in annual payments, or in a combination thereof for costs associated with the installation and maintenance of the defense features on a vessel covered by the contract, as follows:

(A) The costs to build, procure, and install a defense feature in the vessel.

(B) The costs to periodically maintain and test any defense feature on the vessel.

(C) Any increased costs of operation or any loss of revenue attributable to the installation or maintenance of any defense feature on the vessel.

(D) Any additional costs associated with the terms and conditions of the contract.

(E) Payments of such sums as the Government would otherwise expend, if the vessel were placed in the Ready Reserve Fleet, for maintaining the vessel in the status designated as ''ROS–4 status'' in the Ready Reserve Fleet for 25 years.

(3) For any contract under paragraph (1) under which the United States makes advance payments under paragraph (2) for the costs associated with installation or maintenance of any defense feature on a commercial vessel, the contractor shall provide to the United States such security interests in the vessel, by way of a preferred mortgage under section 31322 of title 46 or otherwise, as the head of the agency may prescribe in order to adequately protect the United States against loss for the total amount of those costs.

(4) Each contract entered into under this subsection shall—

(A) set forth terms and conditions under which, so long as a vessel covered by the contract is owned or controlled by the contractor, the contractor is to operate the vessel for the Department of Defense notwithstanding any other contract or commitment of that contractor; and

(B) provide that the contractor operating the vessel for the Department of Defense shall be paid for that operation at fair and reasonable rates.

(5) The head of an agency may not delegate authority under this subsection to any officer or employee in a position below the level of head of a procuring activity.

(6) The head of an agency may not enter into a contract under paragraph (1) that would provide for payments to the contractor as authorized in paragraph (2)(E) until notice of the proposed contract is submitted to the congressional defense committees and a period of 90 days has elapsed.

(k) DEFINITIONS.—In this section:

(1) The term ''Fund'' means the National Defense Sealift Fund established by subsection (a).

(2) The term ''Department of Defense sealift vessel'' means any ship owned, operated, controlled, or chartered by the Department of Defense that is any of the following:

(A) A fast sealift ship, including any vessel in the Fast Sealift Program established under section 1424 of Public Law 101–510 (104 Stat. 1683).

(B) Any other auxiliary vessel that was procured or chartered with specific authorization in law for the vessel, or class of vessels, to be funded in the National Defense Sealift Fund.

(3) The term ''national defense sealift vessel'' means—

(A) a Department of Defense sealift vessel; and

(B) a national defense reserve fleet vessel, including a vessel in the Ready Reserve Force maintained under section 11 of the Merchant Ship Sales Act of 1946 (50 U.S.C. 4405).[1]

(4) The term ''head of an agency'' has the meaning given that term in section 3004 of this title.

(5) The term ''Maritime Security Fleet'' means the fleet established under section 53102(a) of title 46.

(Added Pub. L. 102–484, div. A, title X, §1024(a)(1), Oct. 23, 1992, 106 Stat. 2486; amended Pub. L. 102–396, title V, Oct. 6, 1992, 106 Stat. 1896; Pub. L. 104–106, div. A, title X, §1014(a), title XV, §1502(a)(15), Feb. 10, 1996, 110 Stat. 423, 503; Pub. L. 106–65, div. A, title X, §§1014(b), 1015, 1067(1), Oct. 5, 1999, 113 Stat. 742, 743, 774; Pub. L. 106–398, §1 [[div. A], title X, §1011], Oct. 30, 2000, 114 Stat. 1654, 1654A–251; Pub. L. 107–107, div. A, title X, §1048(e)(9), Dec. 28, 2001, 115 Stat. 1228; Pub. L. 108–136, div. A, title X, §1043(b)(9), Nov. 24, 2003, 117 Stat. 1611; Pub. L. 109–163, div. A, title X, §1018(d), Jan. 6, 2006, 119 Stat. 3426; Pub. L. 109–304, §17(a)(2), Oct. 6, 2006, 120 Stat. 1706; Pub. L. 110–417, [div. A], title XIV, §1407, Oct. 14, 2008, 122 Stat. 4647; Pub. L. 114–328, div. A, title X, §1081(b)(5), Dec. 23, 2016, 130 Stat. 2419; Pub. L. 115–91, div. A, title X, §1021(a)–(c), div. C, title XXXV, §3502(b)(1), Dec. 12, 2017, 131 Stat. 1546, 1547, 1910; Pub. L. 115–232, div. A, title VIII, §809(a), title X, §§1012, 1013, Aug. 13, 2018, 132 Stat. 1840, 1947, 1948; Pub. L. 116–92, div. A, title X, §1031(a), Dec. 20, 2019, 133 Stat. 1579; Pub. L. 116–283, div. A, title X, §1022, title XVIII, §1806(e)(1)(A), Jan. 1, 2021, 134 Stat. 3840, 4155; Pub. L. 118–159, div. A, title X, §1022, Dec. 23, 2024, 138 Stat. 2052.)

Editorial Notes

REFERENCES IN TEXT

Section 11 of the Merchant Ship Sales Act of 1946 (50 U.S.C. 4405), referred to in subsecs. (c)(1)(D) and (k)(3)(B), was redesignated as and transferred to section 57100 of Title 46, Shipping, by Pub. L. 115–91, div. C, title XXXV, §3502(a)(3), Dec. 12, 2017, 131 Stat. 1910.

Section 1424 of Public Law 101–510, referred to in subsecs. (d)(3), (f)(2), and (k)(2)(A), is section 1424 of the National Defense Authorization Act for Fiscal Year 1991, which is set out as a note under section 7291 of this title.

CODIFICATION

Pub. L. 102–396, title V, Oct. 6, 1992, 106 Stat. 1896, provided that section 1024 of the National Defense Authorization Act for Fiscal Year 1993 [H.R. 5006, Pub. L. 102–484], as it passed the Senate on Oct. 3, 1992, shall be amended in subsection 2218(c)(2) proposed for inclusion in this chapter by deleting all after ''expended only'' down to and including ''appropriations Act'' and inserting in lieu thereof ''in amounts authorized by law''. It further provided that for purposes of that amendment, Pub. L. 102–396 shall be treated as having been enacted after Pub. L. 102–484, regardless of the actual dates of enactment. The date of Oct. 3, 1992, referred to as the date the Senate passed the National Defense Authorization Act for Fiscal Year 1993, apparently is based on an order adopted by the Senate on Oct. 3, 1992 [Cong. Rec., vol. 138, pt. 21, p. 30919] providing that when the conference report on the National Defense Authorization Act for Fiscal Year 1993 was received by the Senate from the House of Representatives it would be deemed to have been agreed to. On Oct. 5, 1992, the Senate received the conference report from the House, and it was considered adopted pursuant to that order [Cong. Rec., vol. 138, pt. 22, p. 31565].

AMENDMENTS

2024—Subsec. (f)(3)(A). Pub. L. 118–159, §1022(1)(A), substituted ''subsection (c)(1)(D)'' for ''subsection (c)(1)(E)''.

Subsec. (f)(3)(C). Pub. L. 118–159, §1022(1)(B), substituted ''10'' for ''nine''.

Subsec. (i). Pub. L. 118–159, §1022(2), substituted ''subsection (c)(1)(D)'' for ''subsection (c)(1)(E)''.

2021—Subsec. (f)(3)(C). Pub. L. 116–283, §1022(1), substituted ''nine'' for ''seven''.

Subsec. (f)(3)(E). Pub. L. 116–283, §1022(2)(A), substituted ''four'' for ''two'' in introductory provisions.

Subsec. (f)(3)(E)(ii). Pub. L. 116–283, §1022(2)(B), substituted ''2028'' for ''2026''.

Subsec. (f)(3)(G). Pub. L. 116–283, §1022(3), substituted ''subparagraph (F)'' for ''subparagraph (E)''.

Subsec. (k)(4). Pub. L. 116–283, §1806(e)(1)(A), substituted ''section 3004'' for ''section 2302(1)''.

2019—Subsec. (f)(3)(E)(i). Pub. L. 116–92, §1031(a)(1), substituted ''ten new vessels that are sealift vessels, auxiliary vessels, or a combination of such vessels'' for ''ten new sealift vessels''.

Subsec. (f)(3)(E)(ii). Pub. L. 116–92, §1031(a)(2), struck out ''sealift'' before ''vessels''.

2018—Subsec. (d)(3). Pub. L. 115–232, §809(a), substituted ''section 1424(c) of the National Defense Authorization Act for Fiscal Year 1991 (10 U.S.C. 8661 note)'' for ''section 1424(c) of the National Defense Authorization Act for Fiscal Year 1991 (10 U.S.C. 7291 note)''.

Subsec. (f)(3)(C). Pub. L. 115–232, §1012(1), substituted ''seven'' for ''two'' and ''vessels'' for ''ships''.

Subsec. (f)(3)(E). Pub. L. 115–232, §1012(3), added subpar. (E). Former subpar. (E) redesignated (F).

Subsec. (f)(3)(F). Pub. L. 115–232, §§1012(2), 1013(1)(A), redesignated subpar. (E) as (F) and substituted ''30 days before'' for ''30 days after'' in introductory provisions.

Subsec. (f)(3)(F)(i). Pub. L. 115–232, §1013(1)(B), inserted ''proposed'' before ''date''.

Subsec. (f)(3)(F)(ii). Pub. L. 115–232, §1013(1)(C), substituted ''would be purchased.'' for ''was purchased.''

Subsec. (f)(3)(F)(viii). Pub. L. 115–232, §1013(1)(D), added cl. (viii).

Subsec. (f)(3)(G). Pub. L. 115–232, §1013(2), added subpar. (G).

2017—Subsec. (c)(1)(D), (E). Pub. L. 115–91, §1021(a)(1)(A), redesignated subpar. (E) as (D) and struck out former subpar. (D) which read as follows: ''Research and development relating to national defense sealift.''

Subsec. (c)(3). Pub. L. 115–91, §1021(a)(1)(B), struck out ''or (D)'' after ''subparagraph (B)''.

Subsec. (d)(1)(D). Pub. L. 115–91, §1021(a)(2)(A), struck out subpar. (D) which read as follows: ''research and development relating to national defense sealift.''

Subsec. (d)(4). Pub. L. 115–91, §1021(a)(2)(B), added par. (4).

Subsec. (f)(3). Pub. L. 115–91, §1021(b), added par. (3).

Subsec. (i). Pub. L. 115–91, §3502(b)(1), substituted ''section 57100 of title 46'' for ''section 11 of the Merchant Ship Sales Act of 1946 (50 U.S.C. App. 1744)''.

Subsec. (k)(5). Pub. L. 115–91, §1021(c), added par. (5).

2016—Subsecs. (c)(1)(E), (k)(3)(B). Pub. L. 114–328 substituted ''(50 U.S.C. 4405)'' for ''(50 U.S.C. App. 1744)''.

2008—Subsecs. (j), (k). Pub. L. 110–417, §1407(1), redesignated subsecs. (k) and (*l*) as (j) and (k), respectively, and struck out heading and text of former subsec. (j). Text read as follows: ''Upon a determination by the Secretary of Defense that such action serves the national defense interest and after consultation with the congressional defense committees, the Secretary may use funds available for obligation or expenditure for a purpose specified under subsection (c)(1)(A), (B), (C), and (D) for any purpose under subsection (c)(1).''

Subsec. (k)(2)(B) to (I). Pub. L. 110–417, §1407(2), added subpar. (B) and struck out former subpars. (B) to (I) which read as follows:

''(B) A maritime prepositioning ship.

''(C) An afloat prepositioning ship.

''(D) An aviation maintenance support ship.

''(E) A hospital ship.

''(F) A strategic sealift ship.

''(G) A combat logistics force ship.

''(H) A maritime prepositioned ship.

''(I) Any other auxiliary support vessel.''

Subsec. (*l*). Pub. L. 110–417, §1407(1), redesignated subsec. (*l*) as (k).

2006—Subsec. (d)(2). Pub. L. 109–304 substituted ''sections 57101–57104 and chapter 573 of title 46'' for ''sec-

tions 508 and 510 of the Merchant Marine Act of 1936 (46 U.S.C. App. 1158, 1160), shall be deposited in the Fund''.

Subsec. (f)(1). Pub. L. 109–163 substituted ''A vessel built in a foreign ship yard may not be'' for ''Not more than a total of five vessels built in foreign ship yards may be'' and inserted '', unless specifically authorized by law'' before period at end.

2003—Subsec. (*l*)(4), (5). Pub. L. 108–136 redesignated par. (5) as (4) and struck out former par. (4) which read as follows: ''The term 'congressional defense committees' means—

''(A) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

''(B) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.''

2001—Subsec. (d)(1). Pub. L. 107–107 struck out ''for fiscal years after fiscal year 1993'' after ''Department of Defense'' in introductory provisions.

2000—Subsec. (k)(1). Pub. L. 106–398, §1 [[div. A], title X, §1011(1)], inserted at end ''As consideration for a contract with the head of an agency under this subsection, the company entering into the contract shall agree with the Secretary of Defense to make any vessel covered by the contract available to the Secretary, fully crewed and ready for sea, at any time at any port determined by the Secretary, and for whatever duration the Secretary determines necessary.''

Subsec. (k)(2)(E). Pub. L. 106–398, §1 [[div. A], title X, §1011(2)], added subpar. (E).

Subsec. (k)(6). Pub. L. 106–398, §1 [[div. A], title X, §1011(3)], added par. (6).

1999—Subsec. (k). Pub. L. 106–65, §1015(a)(2), added subsec. (k). Former subsec. (k) redesignated (*l*).

Subsec. (k)(2). Pub. L. 106–65, §1014(b), substituted ''that is any of the following:'' for ''that is—'' in introductory provisions, substituted ''A'' for ''a'' and a period for the semicolon in subpars. (A) and (B), ''An'' for ''an'' and a period for the semicolon in subpar. (C), ''An'' for ''an'' and a period for ''; or'' in subpar. (D), and ''A'' for ''a'' in subpar. (E), and added subpars. (F) to (I).

Subsec. (*l*). Pub. L. 106–65, §1015(a)(1), redesignated subsec. (k) as (*l*).

Subsec. (*l*)(4)(B). Pub. L. 106–65, §1067(1), substituted ''Committee on Armed Services'' for ''Committee on National Security''.

Subsec. (*l*)(5). Pub. L. 106–65, §1015(b), added par. (5).

1996—Subsec. (c)(1). Pub. L. 104–106, §1014(a)(1)(A), substituted ''only for the following purposes:'' for ''only for—''.

Subsec. (c)(1)(A). Pub. L. 104–106, §1014(a)(1)(B), (C), substituted ''Construction'' for ''construction'' and ''vessels.'' for ''vessels;''.

Subsec. (c)(1)(B). Pub. L. 104–106, §1014(a)(1)(B), (C), substituted ''Operation'' for ''operation'' and ''purposes.'' for ''purposes;''.

Subsec. (c)(1)(C). Pub. L. 104–106, §1014(a)(1)(B), (D), substituted ''Installation'' for ''installation'' and ''States.'' for ''States; and''.

Subsec. (c)(1)(D). Pub. L. 104–106, §1014(a)(1)(B), substituted ''Research'' for ''research''.

Subsec. (c)(1)(E). Pub. L. 104–106, §1014(a)(1)(E), added subpar. (E).

Subsec. (i). Pub. L. 104–106, §1014(a)(2), inserted ''(other than subsection (c)(1)(E))'' after ''Nothing in this section''.

Subsec. (j). Pub. L. 104–106, §1502(a)(15)(A), substituted ''the congressional defense committees'' for ''the Committees on Armed Services and on Appropriations of the Senate and the House of Representatives''.

Subsec. (k)(4). Pub. L. 104–106, §1502(a)(15)(B), added par. (4).

1992—Subsec. (c)(2). Pub. L. 102–396 substituted ''in amounts authorized by law'' for ''for programs, projects, and activities and only in amounts authorized in, or otherwise permitted under, an Act other than an appropriations Act''. See Codification note above.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2021 AMENDMENT

Amendment by section 1806(e)(1)(A) of Pub. L. 116–283 effective Jan. 1, 2022, with additional provisions for delayed implementation and applicability of existing law, see section 1801(d) of Pub. L. 116–283, set out as a note preceding section 3001 of this title.

EFFECTIVE DATE OF 2019 AMENDMENT

Pub. L. 116–92, div. A, title X, §1031(b), Dec. 20, 2019, 133 Stat. 1579, provided that: ''The amendments made by subsection (a) [amending this section] shall take effect on October 1, 2019, and shall apply with respect to fiscal years beginning on or after that date.''

EFFECTIVE DATE OF 2018 AMENDMENT

Amendment by section 809(a) of Pub. L. 115–232 effective Feb. 1, 2019, with provision for the coordination of amendments and special rule for certain redesignations, see section 800 of Pub. L. 115–232, set out as a note preceding section 3001 of this title.

TERMINATION OF REPORTING REQUIREMENTS

For termination, effective Dec. 31, 2021, of provisions in subsec. (h) of this section relating to submitting budget requests to Congress, see section 1061 of Pub. L. 114–328, set out as a note under section 111 of this title.

COMPLIANCE BY READY RESERVE FLEET VESSELS WITH SOLAS LIFEBOATS AND FIRE SUPPRESSION REQUIREMENTS

Pub. L. 115–232, div. C, title XXXV, §3502, Aug. 13, 2018, 132 Stat. 2308, provided that: ''The Secretary of Defense shall, consistent with section 2244a of title 10, United States Code, use authority under section 2218 of such title to make such modifications to Ready Reserve Fleet vessels as are necessary for such vessels to comply [with] requirements for lifeboats and fire suppression under the International Convention for the Safety of Life at Sea by not later than October 1, 2021.''

§ 2218a. National Sea-Based Deterrence Fund

(a) ESTABLISHMENT.—There is established in the Treasury of the United States a fund to be known as the ''National Sea-Based Deterrence Fund''.

(b) ADMINISTRATION OF FUND.—The Secretary of Defense shall administer the Fund consistent with the provisions of this section.

(c) FUND PURPOSES.—(1) Funds in the Fund shall be available for obligation and expenditure only for construction (including design of vessels), purchase, alteration, and conversion of national sea-based deterrence vessels.

(2) Funds in the Fund may not be used for a purpose or program unless the purpose or program is authorized by law.

(d) DEPOSITS.—There shall be deposited in the Fund all funds appropriated to the Department of Defense for construction (including design of vessels), purchase, alteration, and conversion of national sea-based deterrence vessels.

(e) EXPIRATION OF FUNDS AFTER 5 YEARS.—No part of an appropriation that is deposited in the Fund pursuant to subsection (d) shall remain available for obligation more than five years after the end of fiscal year for which appropriated except to the extent specifically provided by law.

(f) AUTHORITY TO ENTER INTO ECONOMIC ORDER QUANTITY CONTRACTS.—(1) The Secretary of the Navy may use funds deposited in the Fund to enter into contracts known as ''economic order

quantity contracts'' with private shipyards and other commercial or government entities to achieve economic efficiencies based on production economies for major components or subsystems. The authority under this subsection extends to the procurement of parts, components, and systems (including weapon systems) common with and required for other nuclear powered vessels under joint economic order quantity contracts.

(2) A contract entered into under paragraph (1) shall provide that any obligation of the United States to make a payment under the contract is subject to the availability of appropriations for that purpose, and that total liability to the Government for termination of any contract entered into shall be limited to the total amount of funding obligated at time of termination.

(g) AUTHORITY TO BEGIN MANUFACTURING AND FABRICATION EFFORTS PRIOR TO SHIP AUTHORIZATION.—(1) The Secretary of the Navy may use funds deposited into the Fund to enter into contracts for advance construction of national sea-based deterrence vessels to support achieving cost savings through workload management, manufacturing efficiencies, or workforce stability, or to phase fabrication activities within shipyard and manage sub-tier manufacturer capacity.

(2) A contract entered into under paragraph (1) shall provide that any obligation of the United States to make a payment under the contract is subject to the availability of appropriations for that purpose, and that total liability to the Government for termination of any contract entered into shall be limited to the total amount of funding obligated at time of termination.

(h) AUTHORITY TO USE INCREMENTAL FUNDING TO ENTER INTO CONTRACTS FOR CERTAIN ITEMS.—(1) The Secretary of the Navy may use funds deposited into the Fund to enter into incrementally funded contracts for—

(A) advance procurement of high value, long lead time items for nuclear powered vessels to better support construction schedules and achieve cost savings through schedule reductions and properly phased installment payments; and

(B) construction of the first two Columbia class submarines.

(2) A contract entered into under paragraph (1) shall provide that any obligation of the United States to make a payment under the contract is subject to the availability of appropriations for that purpose, and that total liability to the Government for termination of any contract entered into shall be limited to the total amount of funding obligated at time of termination.

(i) AUTHORITY FOR MULTIYEAR PROCUREMENT OF CRITICAL COMPONENTS TO SUPPORT CONTINUOUS PRODUCTION.—(1) To implement the continuous production of critical components, the Secretary of the Navy may use funds deposited in the Fund, in conjunction with funds appropriated for the procurement of other nuclear-powered vessels, to enter into one or more multiyear contracts (including economic ordering quantity contracts), for the procurement of critical contractor-furnished and Government-furnished components for critical components of national sea-based deterrence vessels. The authority under this subsection extends to the procurement of equivalent critical components common with and required for other nuclear-powered vessels.

(2) In each annual budget request submitted to Congress, the Secretary shall clearly identify funds requested for critical components and the individual ships and programs for which such funds are requested.

(3) Any contract entered into pursuant to paragraph (1) shall provide that any obligation of the United States to make a payment under the contract is subject to the availability of appropriations for that purpose and that the total liability to the Government for the termination of the contract shall be limited to the total amount of funding obligated for the contract as of the date of the termination.

(j) BUDGET REQUESTS.—Budget requests submitted to Congress for the Fund shall separately identify the amount requested for programs, projects, and activities for construction (including design of vessels), purchase, alteration, and conversion of national sea-based deterrence vessels.

(k) DEFINITIONS.—In this section:

(1) The term ''Fund'' means the National Sea-Based Deterrence Fund established by subsection (a).

(2) The term ''national sea-based deterrence vessel'' means any submersible vessel constructed or purchased after fiscal year 2016 that is owned, operated, or controlled by the Department of Defense and that carries operational intercontinental ballistic missiles.

(3) The term ''critical component'' means any of the following:

(A) A common missile compartment component.
(B) A spherical air flask.
(C) An air induction diesel exhaust valve.
(D) An auxiliary seawater valve.
(E) A hovering valve.
(F) A missile compensation valve.
(G) A main seawater valve.
(H) A launch tube.
(I) A trash disposal unit.
(J) A logistics escape trunk.
(K) A torpedo tube.
(L) A weapons shipping cradle weldment.
(M) A control surface.
(N) A launcher component.
(O) A propulsor.
(P) Major bulkheads and tanks.
(Q) All major pumps and motors.
(R) Large vertical array.
(S) Atmosphere control equipment.
(T) Diesel systems and components.
(U) Hydraulic valves and components.
(V) Bearings.
(W) Major air and blow valves and components.
(X) Decks and superstructure.
(Y) Castings, forgings, and tank structure.
(Z) Hatches and hull penetrators.

(Added Pub. L. 113–291, div. A, title X, §1022(a)(1), Dec. 19, 2014, 128 Stat. 3486; amended Pub. L. 114–92, div. A, title X, §1022(a), Nov. 25, 2015, 129 Stat. 965; Pub. L. 114–328, div. A, title X, §1023, Dec. 23, 2016, 130 Stat. 2388; Pub. L. 115–91, div. A, title X, §1022, Dec. 12, 2017, 131 Stat. 1548;

Pub. L. 116–283, div. A, title X, §1023(a), Jan. 1, 2021, 134 Stat. 3840; Pub. L. 118–31, div. A, title X, §1016, Dec. 22, 2023, 137 Stat. 382.)

Editorial Notes

AMENDMENTS

2023—Subsec. (k)(3)(P) to (Z). Pub. L. 118–31 added subpars. (P) to (Z).

2021—Subsec. (h)(1). Pub. L. 116–283 substituted ''incrementally funded contracts for—'' for ''incrementally funded contracts for advance procurement of high value, long lead time items for nuclear powered vessels to better support construction schedules and achieve cost savings through schedule reductions and properly phased installment payments.'' and added subpars. (A) and (B).

2017—Subsec. (i). Pub. L. 115–91, §1022(c), struck out ''of the Common Missile Compartment'' after ''Continuous Production'' in heading.

Subsec. (i)(1). Pub. L. 115–91, §1022(a)(2), substituted ''equivalent critical components'' for ''equivalent critical parts, components, systems, and subsystems''.

Pub. L. 115–91, §1022(a)(1), which directed the substitution of ''critical components'' for ''the common missile compartment'' wherever appearing, was executed by making the substitution for ''the common missile compartment'' the first time appearing and for ''the common missile compartments'' the second time appearing, to reflect the probable intent of Congress.

Subsec. (i)(2). Pub. L. 115–91, §1022(a)(1), substituted ''critical components'' for ''the common missile compartment''.

Subsec. (k)(3). Pub. L. 115–91, §1022(b), added par. (3).

2016—Subsecs. (i), (j). Pub. L. 114–328, §1023(a), added subsec. (i) and redesignated former subsec. (i) as (j). Former subsec. (j) redesignated (k).

Subsec. (k). Pub. L. 114–328, §1023(a)(1), redesignated subsec. (j) as (k).

Subsec. (k)(2). Pub. L. 114–328, §1023(b), substituted ''any submersible vessel constructed or purchased after fiscal year 2016 that is'' for ''any vessel'' and inserted ''and'' before ''that carries''.

2015—Subsecs. (f) to (j). Pub. L. 114–92 added subsecs. (f) to (h) and redesignated former subsecs. (f) and (g) as (i) and (j), respectively.

§ 2219. Grants for improvement of Navy ship repair or alterations capability

(a) ASSISTANCE AUTHORIZED.—(1) Subject to the availability of appropriations, the Secretary of the Navy may make grants to an eligible entity for the purpose of carrying out—

(A) a capital improvement project; or

(B) a maritime training program designed to foster technical skills and operational productivity.

(2) The amount of a grant under this section may not exceed 75 percent of the total cost of the project or program funded by the grant.

(3) A grant provided under this section may not be used to construct buildings or other physical facilities, except for piers, dry docks, and structures in support of piers and dry docks, or to acquire land.

(4) The Secretary may not award a grant to an eligible entity under this section unless the Secretary determines that—

(A) the entity has access to sufficient non-Federal funding to meet the requirement under paragraph (2);

(B) the entity has authority to carry out the proposed project; and

(C) the project or program would improve—

(i) efficiency, competitive operations, capability, or quality of United States Navy ship repair or alterations; or

(ii) employee, or potential employee, skills and enhanced productivity related to United States Navy ship repair or alterations.

(b) ELIGIBILITY.—To be eligible for a grant under this section, an entity shall—

(1) be a shipyard or other entity that provides ship repair or alteration for non-nuclear ships;

(2) submit an application, at such time, in such form, and containing such information and assurances as the Secretary may require, including a comprehensive description of—

(A) the need for the project or program proposed to be funded under the grant;

(B) the methodology to be used to implement the project or program; and

(C) any existing programs or arrangements that could be used to supplement or leverage a grant provided under this section; and

(3) enter into an agreement with the Secretary under which the entity agrees—

(A) to complete the project or program funded by the grant within a certain timeframe and without unreasonable delay and the Secretary determines such project or program is likely to be completed within the timeframe provided in such agreement;

(B) to return to the Secretary any amount of the grant that is—

(i) not used by the grant recipient for the purpose for which the grant was awarded; or

(ii) not obligated or expended within the timeframe provided in the agreement;

(C) to maintain such records as the Secretary may require and make such records available for review and audit by the Secretary; and

(D) not to purchase any product or material for the project or program using grant funds, including any commercially available off-the-shelf item, unless such product or material is—

(i) an unmanufactured article, material, or supply that has been mined or produced in the United States; or

(ii) a manufactured article, material, or supply that has been manufactured in the United States substantially all from articles, materials, or supplies mined, produced, or manufactured in the United States.

(c) GUIDELINES.—The Secretary shall issue guidelines to establish appropriate accounting, reporting, and review procedures to ensure that—

(1) amounts awarded as grants under this section are used for the purposes for which such amounts were made available; and

(2) an entity that receives a grant under this section complies with the terms of the agreement such entity enters into with the Secretary pursuant to subsection (b)(3).

(d) DEFINITIONS.—In this section:

(1) The term ''commercially available off-the-shelf item''—

(A) means any item of supply (including construction material) that is—

(i) a commercial item, as defined by section 2.101 of title 48, Code of Federal Regu-

lations (as in effect on the date of the enactment of the National Defense Authorization Act for Fiscal Year 2024); and

(ii) sold in substantial quantities in the commercial marketplace; and

(B) does not include bulk cargo, as defined in section 40102(4) of title 46, such as agricultural products and petroleum products.

(2) The term ''product or material'', with respect to a project or program—

(A) means an article, material, or supply brought to the site where the project or program is being carried out for incorporation into the project or program; and

(B) includes an item brought to the site preassembled from articles, materials, or supplies.

(3) The term ''United States'' includes the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, Guam, American Samoa, and the Virgin Islands.

(Added Pub. L. 118–31, div. A, title X, § 1017, Dec. 22, 2023, 137 Stat. 382.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of the National Defense Authorization Act for Fiscal Year 2024, referred to in subsec. (d)(1)(A)(i), is the date of enactment of Pub. L. 118–31, which was approved Dec. 22, 2023.

PRIOR PROVISIONS

A prior section 2219 was renumbered section 2491c of this title.

§ 2220. Performance based management: acquisition programs

(a) ESTABLISHMENT OF GOALS.—The Secretary of Defense shall approve or define the cost, performance, and schedule goals for major defense acquisition programs of the Department of Defense and for each phase of the acquisition cycle of such programs.

(b) EVALUATION OF COST GOALS.—The Under Secretary of Defense (Comptroller) shall evaluate the cost goals proposed for each major defense acquisition program of the Department.

(c) SUNSET.—The authority under this section shall terminate on September 30, 2018.

(Added Pub. L. 103–355, title V, § 5001(a)(1), Oct. 13, 1994, 108 Stat. 3349; amended Pub. L. 104–106, div. A, title XV, § 1503(a)(20), div. D, title XLIII, § 4321(b)(1), Feb. 10, 1996, 110 Stat. 512, 671; Pub. L. 105–85, div. A, title VIII, § 841(a), Nov. 18, 1997, 111 Stat. 1843; Pub. L. 107–314, div. A, title X, § 1041(a)(8), Dec. 2, 2002, 116 Stat. 2645; Pub. L. 114–328, div. A, title VIII, § 833(a)(2), Dec. 23, 2016, 130 Stat. 2283.)

Editorial Notes

AMENDMENTS

2016—Subsec. (c). Pub. L. 114–328 added subsec. (c).

2002—Subsec. (a). Pub. L. 107–314, § 1041(a)(8)(B), (C), struck out par. (1) designation and redesignated par. (2) as subsec. (b).

Subsec. (b). Pub. L. 107–314, § 1041(a)(8)(A), (C), redesignated subsec. (a)(2) as (b) and struck out heading and text of former subsec. (b). Text read as follows: ''The Secretary of Defense shall include in the annual report submitted to Congress pursuant to section 113(c) of this title an assessment of whether major acquisition programs of the Department of Defense are achieving, on average, 90 percent of cost, performance, and schedule goals established pursuant to subsection (a) and whether the average period for converting emerging technology into operational capability has decreased by 50 percent or more from the average period required for such conversion as of October 13, 1994. The Secretary shall use data from existing management systems in making the assessment.''

Subsec. (c). Pub. L. 107–314, § 1041(a)(8)(A), struck out heading and text of subsec. (c). Text read as follows: ''Whenever the Secretary of Defense, in the assessment required by subsection (b), determines that major defense acquisition programs of the Department of Defense are not achieving, on average, 90 percent of cost, performance, and schedule goals established pursuant to subsection (a), the Secretary shall ensure that there is a timely review of major defense acquisition programs and other programs as appropriate. In conducting the review, the Secretary shall—

''(1) determine whether there is a continuing need for programs that are significantly behind schedule, over budget, or not in compliance with performance or capability requirements; and

''(2) identify suitable actions to be taken, including termination, with respect to such programs.''

1997—Subsec. (b). Pub. L. 105–85 substituted ''whether major acquisition programs'' for ''whether major and nonmajor acquisition programs''.

1996—Subsec. (a)(2). Pub. L. 104–106, § 1503(a)(20), substituted ''Under Secretary of Defense (Comptroller)'' for ''Comptroller of the Department of Defense''.

Subsec. (b). Pub. L. 104–106, § 4321(b)(1), substituted ''October 13, 1994'' for ''the date of the enactment of the Federal Acquisition Streamlining Act of 1994''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 1996 AMENDMENT

Pub. L. 104–106, div. D, title XLIV, § 4401, Feb. 10, 1996, 110 Stat. 678, provided that:

''(a) EFFECTIVE DATE.—Except as otherwise provided in this division [div. D (§§ 4001–4402) of Pub. L. 104–106, see Tables for classification], this division and the amendments made by this division shall take effect on the date of the enactment of this Act [Feb. 10, 1996].

''(b) APPLICABILITY OF AMENDMENTS.—

''(1) SOLICITATIONS, UNSOLICITED PROPOSALS, AND RELATED CONTRACTS.—An amendment made by this division shall apply, in the manner prescribed in the final regulations promulgated pursuant to section 4402 [110 Stat. 678] to implement such amendment, with respect to any solicitation that is issued, any unsolicited proposal that is received, and any contract entered into pursuant to such a solicitation or proposal, on or after the date described in paragraph (3).

''(2) OTHER MATTERS.—An amendment made by this division shall also apply, to the extent and in the manner prescribed in the final regulations promulgated pursuant to section 4402 to implement such amendment, with respect to any matter related to—

''(A) a contract that is in effect on the date described in paragraph (3);

''(B) an offer under consideration on the date described in paragraph (3); or

''(C) any other proceeding or action that is ongoing on the date described in paragraph (3).

''(3) DEMARCATION DATE.—The date referred to in paragraphs (1) and (2) is the date specified in such final regulations. The date so specified shall be January 1, 1997, or any earlier date that is not within 30

days after the date on which such final regulations are published.''

PILOT PROGRAMS FOR TESTING PROGRAM MANAGER PERFORMANCE OF PRODUCT SUPPORT OVERSIGHT RESPONSIBILITIES FOR LIFE CYCLE OF ACQUISITION PROGRAMS

Pub. L. 105–261, div. A, title VIII, §816, Oct. 17, 1998, 112 Stat. 2088, authorized the Secretary of Defense to designate 10 acquisition programs of the military departments as pilot programs on program manager responsibility for product support and required report to Congress by Feb. 1, 1999.

ENHANCED SYSTEM OF PERFORMANCE INCENTIVES

Pub. L. 103–355, title V, §5001(b), Oct. 13, 1994, 108 Stat. 3350, provided that, within one year after Oct. 13, 1994, the Secretary of Defense should review the incentives and personnel actions available for encouraging excellence in the management of defense acquisition programs and provide an enhanced system of incentives, including pay for performance, to facilitate the achievement of goals approved or defined pursuant to subsec. (a) of this section.

RECOMMENDED LEGISLATION

Pub. L. 103–355, title V, §5001(c), Oct. 13, 1994, 108 Stat. 3350, directed the Secretary of Defense, not later than one year after Oct 13, 1994, to submit to Congress any recommended legislation that the Secretary considered necessary to carry out this section and otherwise to facilitate and enhance management of Department of Defense acquisition programs on the basis of performance.

[§ 2221. Repealed. Pub. L. 105–261, div. A, title IX, § 906(f)(1), Oct. 17, 1998, 112 Stat. 2096]

Section, added Pub. L. 104–106, div. A, title IX, §914(a)(1), Feb. 10, 1996, 110 Stat. 412; amended Pub. L. 104–201, div. A, title X, §1008(a), Sept. 23, 1996, 110 Stat. 2633; Pub. L. 105–85, div. A, title X, §1006(a), Nov. 18, 1997, 111 Stat. 1869; Pub. L. 105–261, div. A, title X, §1069(b)(2), Oct. 17, 1998, 112 Stat. 2136, related to Fisher House trust funds. See section 2493 of this title.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF REPEAL

Repeal effective 90 days after Oct. 17, 1998, see section 906(f)(3) of Pub. L. 105–261, set out as an Effective Date of 1998 Amendment note under section 1321 of Title 31, Money and Finance.

§ 2222. Defense business systems: business process reengineering; enterprise architecture; management

(a) DEFENSE BUSINESS PROCESSES GENERALLY.—The Secretary of Defense shall ensure that defense business processes are reviewed, and as appropriate revised, through business process reengineering to match best commercial practices, to the maximum extent practicable, so as to minimize customization of commercial business systems.

(b) DEFENSE BUSINESS SYSTEMS GENERALLY.—The Secretary of Defense shall ensure that each covered defense business system developed, deployed, and operated by the Department of Defense—

(1) supports efficient business processes that have been reviewed, and as appropriate revised, through business process reengineering;

(2) is integrated into a comprehensive defense business enterprise architecture;

(3) is managed in a manner that provides visibility into, and traceability of, expenditures for the system; and

(4) uses an acquisition and sustainment strategy that prioritizes the use of commercial software and business practices.

(c) ISSUANCE OF GUIDANCE.—

(1) SECRETARY OF DEFENSE GUIDANCE.—The Secretary shall issue guidance to provide for the coordination of, and decision making for, the planning, programming, and control of investments in covered defense business systems.

(2) SUPPORTING GUIDANCE.—The Secretary shall direct the Chief Information Officer of the Department of Defense, the Under Secretary of Defense for Acquisition and Sustainment, and the Chief Information Officer of each of the military departments to issue and maintain supporting guidance, as appropriate and within their respective areas of responsibility, for the guidance of the Secretary issued under paragraph (1).

(d) GUIDANCE ELEMENTS.—The guidance issued under subsection (c) shall include the following elements:

(1) Policy to ensure that the business processes of the Department of Defense are continuously reviewed and revised—

(A) to implement the most streamlined and efficient business processes practicable; and

(B) to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet or incorporate requirements or interfaces that are unique to the Department of Defense.

(2) A process to establish requirements for covered defense business systems.

(3) Mechanisms for the planning and control of investments in covered defense business systems, including a process for the collection and review of programming and budgeting information for covered defense business systems.

(4) Policy requiring the periodic review of covered defense business systems that have been fully deployed, by portfolio, to ensure that investments in such portfolios are appropriate.

(5) Policy to ensure full consideration of sustainability and technological refreshment requirements, and the appropriate use of open architectures.

(6) Policy to ensure that best acquisition and systems engineering practices are used in the procurement and deployment of commercial systems, modified commercial systems, and defense-unique systems to meet Department of Defense missions.

(7) Policy to ensure a covered defense business system is in compliance with the Department's auditability requirements.

(8) Policy to ensure approvals required for the development of a covered defense business system.

(e) DEFENSE BUSINESS ENTERPRISE ARCHITECTURE.—

(1) BLUEPRINT.—The Secretary, working through the Chief Information Officer of the Department of Defense, shall develop and maintain a blueprint to guide the development

of integrated business processes within the Department of Defense. Such blueprint shall be known as the ''defense business enterprise architecture''.

(2) PURPOSE.—The defense business enterprise architecture shall be sufficiently defined to effectively guide implementation of interoperable defense business system solutions and shall be consistent with the policies and procedures established by the Director of the Office of Management and Budget.

(3) ELEMENTS.—The defense business enterprise architecture shall—

(A) include policies, procedures, business data standards, business performance measures, and business information requirements that apply uniformly throughout the Department of Defense; and

(B) enable the Department of Defense to—

(i) comply with all applicable law, including Federal accounting, financial management, and reporting requirements;

(ii) routinely produce verifiable, timely, accurate, and reliable business and financial information for management purposes;

(iii) integrate budget, accounting, and program information and systems; and

(iv) identify whether each existing business system is a part of the business systems environment outlined by the defense business enterprise architecture, will become a part of that environment with appropriate modifications, or is not a part of that environment.

(4) INTEGRATION INTO INFORMATION TECHNOLOGY ARCHITECTURE.—(A) The defense business enterprise architecture shall be integrated into the information technology enterprise architecture required under subparagraph (B).

(B) The Chief Information Officer of the Department of Defense shall develop an information technology enterprise architecture. The architecture shall describe a plan for improving the information technology and computing infrastructure of the Department of Defense, including for each of the major business processes conducted by the Department of Defense.

(5) COMMON ENTERPRISE DATA.—The defense business enterprise shall include enterprise data that may be automatically extracted from the relevant systems to facilitate Department of Defense-wide analysis and management of its business operations.

(6) ROLES AND RESPONSIBILITIES.—

(A) The Chief Information Officer of the Department of Defense, in coordination with the Chief Data and Artificial Intelligence Officer, shall have primary decision-making authority with respect to the development of common enterprise data. In consultation with the Defense Business Council, the Chief Information Officer shall—

(i) develop an associated data governance process; and

(ii) oversee the preparation, extraction, and provision of data across the defense business enterprise.

(B) The Chief Information Officer and the Under Secretary of Defense (Comptroller) shall—

(i) in consultation with the Defense Business Council, document and maintain any common enterprise data for their respective areas of authority;

(ii) participate in any related data governance process;

(iii) extract data from defense business systems as needed to support priority activities and analyses;

(iv) when appropriate, ensure the source data is the same as that used to produce the financial statements subject to annual audit;

(v) in consultation with the Defense Business Council, provide access, except as otherwise provided by law or regulation, to such data to the Office of the Secretary of Defense, the Joint Staff, the military departments, the combatant commands, the Defense Agencies, the Department of Defense Field Activities, and all other offices, agencies, activities, and commands of the Department of Defense; and

(vi) ensure consistency of the common enterprise data maintained by their respective organizations.

(C) The Director of Cost Assessment and Program Evaluation shall have access to data for the purpose of executing missions as designated by the Secretary of Defense.

(D) The Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the Secretaries of the military departments, commanders of combatant commands, the heads of the Defense Agencies, the heads of the Department of Defense Field Activities, and the heads of all other offices, agencies, activities, and commands of the Department of Defense shall provide access to the relevant system of such department, combatant command, Defense Agency, Defense Field Activity, or office, agency, activity, and command organization, as applicable, and data extracted from such system, for purposes of automatically populating data sets coded with common enterprise data.

(f) DEFENSE BUSINESS COUNCIL.—

(1) REQUIREMENT FOR COUNCIL.—The Secretary shall establish a Defense Business Council to provide advice to the Secretary on developing the defense business enterprise architecture, reengineering the Department's business processes, developing and deploying defense business systems, and developing requirements for defense business systems. The Council shall be co-chaired by the Chief Information Officer and the Performance Improvement Officer of the Department of Defense.

(2) MEMBERSHIP.—The membership of the Council shall include the following:

(A) The Chief Information Officers of the military departments, or their designees.

(B) The Chief Management Officers of the military departments, or their designees.

(C) The following officials of the Department of Defense, or their designees:

(i) The Under Secretary of Defense for Acquisition and Sustainment with respect to acquisition, logistics, and installations management processes.

(ii) The Under Secretary of Defense (Comptroller) with respect to financial management and planning and budgeting processes.

(iii) The Under Secretary of Defense for Personnel and Readiness with respect to human resources management processes.

(iv) The Chief Data and Artificial Intelligence Officer of the Department of Defense.

(g) APPROVALS REQUIRED FOR DEVELOPMENT.—(1) INITIAL APPROVAL REQUIRED.—The Secretary shall ensure that a covered defense business system program cannot proceed into development (or, if no development is required, into production or fielding) unless the appropriate approval official (as specified in paragraph (2)) determines that—

(A) the system has been, or is being, reengineered to be as streamlined and efficient as practicable, and the implementation of the system will maximize the elimination of unique software requirements and unique interfaces;

(B) the system and business system portfolio are or will be in compliance with the defense business enterprise architecture developed pursuant to subsection (e) or will be in compliance as a result of modifications planned;

(C) the system has valid, achievable requirements and a viable plan for implementing those requirements (including, as appropriate, market research, business process reengineering, and prototyping activities);

(D) the system has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and

(E) the system is in compliance with the Department's auditability requirements.

(2) APPROPRIATE OFFICIAL.—For purposes of paragraph (1), the appropriate approval official with respect to a covered defense business system is the following:

(A) Except as may be provided in subparagraph (C), in the case of a priority defense business system, the Chief Information Officer of the Department of Defense.

(B) Except as may be provided in subparagraph (C), for any defense business system other than a priority defense business system—

(i) in the case of a system of a military department, the Chief Information Officer of that military department; and

(ii) in the case of a system of a Defense Agency or Department of Defense Field Activity, or a system that will support the business process of more than one military department or Defense Agency or Department of Defense Field Activity, the Chief Information Officer of the Department of Defense.

(C) In the case of any defense business system, such official other than the applicable official under subparagraph (A) or (B) as the Secretary designates for such purpose.

(3) ANNUAL CERTIFICATION.—For any fiscal year in which funds are expended for development or sustainment pursuant to a covered defense business system program, the appropriate approval official shall review the system and certify, certify with conditions, or decline to certify, as the case may be, that it continues to satisfy the requirements of paragraph (1). If the approval official determines that certification cannot be granted, the approval official shall notify the milestone decision authority for the program and provide a recommendation for corrective action.

(4) OBLIGATION OF FUNDS IN VIOLATION OF REQUIREMENTS.—The obligation of Department of Defense funds for a covered defense business system program that has not been certified in accordance with paragraph (3) is a violation of section 1341(a)(1)(A) of title 31.

(h) RESPONSIBILITY OF MILESTONE DECISION AUTHORITY.—The milestone decision authority for a covered defense business system program shall be responsible for the acquisition of such system and shall ensure that acquisition process approvals are not considered for such system until the relevant certifications and approvals have been made under this section.

(i) DEFINITIONS.—In this section:

(1)(A) DEFENSE BUSINESS SYSTEM.—The term ''defense business system'' means an information system that is operated by, for, or on behalf of the Department of Defense, including any of the following:

(i) A financial system.

(ii) A financial data feeder system.

(iii) A contracting system.

(iv) A logistics system.

(v) A planning and budgeting system.

(vi) An installations management system.

(vii) A human resources management system.

(viii) A training and readiness system.

(B) The term does not include—

(i) a national security system; or

(ii) an information system used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the Department of Defense conducted for the morale, welfare, and recreation of members of the armed forces using nonappropriated funds.

(2) COVERED DEFENSE BUSINESS SYSTEM.—The term ''covered defense business system'' means a defense business system that is expected to have a total amount of budget authority, over the period of the current future-years defense program submitted to Congress under section 221 of this title, in excess of $50,000,000.

(3) BUSINESS SYSTEM PORTFOLIO.—The term ''business system portfolio'' means all business systems performing functions closely related to the functions performed or to be performed by a covered defense business system.

(4) COVERED DEFENSE BUSINESS SYSTEM PROGRAM.—The term ''covered defense business system program'' means a defense acquisition

program to develop and field a covered defense business system or an increment of a covered defense business system.

(5) PRIORITY DEFENSE BUSINESS SYSTEM.—The term ''priority defense business system'' means a defense business system that is—

(A) expected to have a total amount of budget authority over the period of the current future-years defense program submitted to Congress under section 221 of this title in excess of $250,000,000; or

(B) designated by the Chief Information Officer of the Department of Defense as a priority defense business system, based on specific program analyses of factors including complexity, scope, and technical risk, and after notification to Congress of such designation.

(6) ENTERPRISE ARCHITECTURE.—The term ''enterprise architecture'' has the meaning given that term in section 3601(4) of title 44.

(7) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term in section 11101 of title 40, United States Code.

(8) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given that term in section 3552(b)(6)(A) of title 44.

(9) BUSINESS PROCESS MAPPING.—The term ''business process mapping'' means a procedure in which the steps in a business process are clarified and documented in both written form and in a flow chart.

(10) COMMON ENTERPRISE DATA.—The term ''common enterprise data'' means business operations or management-related data, generally from defense business systems, in a usable format that is automatically accessible by authorized personnel and organizations.

(11) DATA GOVERNANCE PROCESS.—The term ''data governance process'' means a system to manage the timely Department of Defense-wide sharing of data described under subsection (e)(6)(A).

(Added Pub. L. 108–375, div. A, title III, §332(a)(1), Oct. 28, 2004, 118 Stat. 1851; amended Pub. L. 109–364, div. A, title IX, §906(a), Oct. 17, 2006, 120 Stat. 2354; Pub. L. 110–417, [div. A], title III, §351, Oct. 14, 2008, 122 Stat. 4425; Pub. L. 111–84, div. A, title X, §1072(a), Oct. 28, 2009, 123 Stat. 2470; Pub. L. 111–383, div. A, title X, §1075(b)(29), Jan. 7, 2011, 124 Stat. 4370; Pub. L. 112–81, div. A, title IX, §901, Dec. 31, 2011, 125 Stat. 1527; Pub. L. 112–239, div. A, title IX, §906, Jan. 2, 2013, 126 Stat. 1869; Pub. L. 113–66, div. A, title IX, §901, Dec. 26, 2013, 127 Stat. 815; Pub. L. 113–283, §2(e)(5)(A), Dec. 18, 2014, 128 Stat. 3087; Pub. L. 113–291, div. A, title VIII, §803, title IX, §901(d), (k)(3), title X, §1071(f)(16), Dec. 19, 2014, 128 Stat. 3427, 3463, 3468, 3511; Pub. L. 114–92, div. A, title VIII, §883(a)(1), (f), title X, §1081(a)(7), Nov. 25, 2015, 129 Stat. 942, 1001; Pub. L. 114–328, div. A, title X, §1081(a)(6), (c)(5), Dec. 23, 2016, 130 Stat. 2417, 2419; Pub. L. 115–91, div. A, title IX, §912(a), title X, §1081(b)(2), Dec. 12, 2017, 131 Stat. 1519, 1597; Pub. L. 115–232, div. A, title X, §1081(f)(1)(A)(ii), Aug. 13, 2018, 132 Stat. 1986; Pub. L. 116–92, div. A, title VIII, §839(a), title IX, §902(25), title XVII, §1731(a)(31), Dec. 20, 2019, 133 Stat. 1498, 1545, 1814; Pub. L. 117–263, div. A, title IX, §902, Dec. 23, 2022, 136 Stat. 2748; Pub. L. 118–159, div. A, title IX, §902(b), Dec. 23, 2024, 138 Stat. 2026.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2222, added Pub. L. 105–85, div. A, title X, §1008(a)(1), Nov. 18, 1997, 111 Stat. 1870; amended Pub. L. 107–107, div. A, title X, §1009(b)(1)–(3)(A), Dec. 28, 2001, 115 Stat. 1208, 1209, required Secretary of Defense to submit to Congress an annual strategic plan for improvement of financial management within Department of Defense and specified statements and matters to be included in the plan, prior to repeal by Pub. L. 107–314, div. A, title X, §1004(h)(1), Dec. 2, 2002, 116 Stat. 2631.

AMENDMENTS

2024—Subsec. (f)(1). Pub. L. 118–159 substituted ''co-chaired'' for ''chaired'' and inserted ''and the Performance Improvement Officer'' after ''Chief Information Officer''.

2022—Subsec. (c)(2). Pub. L. 117–263, §902(1), substituted ''the Chief Information Officer of the Department of Defense, the Under Secretary of Defense for Acquisition and Sustainment, and the Chief Information Officer'' for ''the Chief Management Officer of the Department of Defense, the Under Secretary of Defense for Acquisition and Sustainment, the Chief Information Officer, and the Chief Management Officer''.

Subsec. (e)(1). Pub. L. 117–263, §902(2)(A), substituted ''the Chief Information Officer'' for ''the Chief Management Officer''.

Subsec. (e)(6)(A). Pub. L. 117–263, §902(2)(B)(i), in introductory provisions, substituted ''The Chief Information Officer of the Department of Defense, in coordination with the Chief Data and Artificial Intelligence Officer,'' for ''The Chief Management Officer of the Department of Defense'' and ''the Chief Information Officer shall—'' for ''the Chief Management Officer shall—''.

Subsec. (e)(6)(B). Pub. L. 117–263, §902(2)(B)(ii), substituted ''The Chief Information Officer'' for '' The Chief Management Officer'' in introductory provisions.

Subsec. (f)(1). Pub. L. 117–263, §902(3)(A), struck out ''the Chief Management Officer and'' before ''the Chief Information Officer''.

Subsec. (f)(2). Pub. L. 117–263, §902(3)(B)(i), (ii), added subpar. (A) and redesignated former subpars. (A) and (B) as (B) and (C), respectively.

Subsec. (f)(2)(C)(iv). Pub. L. 117–263, §902(3)(B)(iii), added cl. (iv).

Subsec. (g)(2). Pub. L. 117–263, §902(4), substituted ''the Chief Information Officer'' for ''the Chief Management Officer'' wherever appearing.

Subsec. (i)(5)(B). Pub. L. 117–263, §902(5), substituted ''the Chief Information Officer'' for ''the Chief Management Officer''.

2019—Subsec. (c)(2). Pub. L. 116–92, §902(25)(A), substituted ''Under Secretary of Defense for Acquisition and Sustainment'' for ''Under Secretary of Defense for Acquisition, Technology, and Logistics''.

Subsec. (d). Pub. L. 116–92, §839(a)(1), substituted ''subsection (c)'' for ''subsection (c)(1)'' in introductory provisions.

Subsec. (d)(7), (8). Pub. L. 116–92, §839(a)(2), added pars. (7) and (8).

Subsec. (f)(2)(B)(i). Pub. L. 116–92, §902(25)(B), substituted ''Under Secretary of Defense for Acquisition and Sustainment'' for ''Under Secretary of Defense for Acquisition, Technology, and Logistics''.

Subsec. (i)(11). Pub. L. 116–92, §1731(a)(31), substituted ''subsection (e)(6)(A)'' for ''subsection (a)(6)(A)''.

2018—Pub. L. 115–232 substituted ''Chief Management Officer'' for ''Deputy Chief Management Officer'' in subsec. (c)(2) after ''shall direct the'' and in subsecs. (e)(1), (f)(1), (g)(2)(A), (B)(ii), and (i)(5)(B).

2017—Subsecs. (c)(2), (e)(1). Pub. L. 115–91, §1081(b)(2), repealed Pub. L. 114–92, §883(f)(1)(A). See 2015 Amendment notes below.

Subsec. (e)(5), (6). Pub. L. 115–91, §912(a)(1), added pars. (5) and (6).

Subsec. (f)(1). Pub. L. 115–91, §1081(b)(2), repealed Pub. L. 114–92, §883(f)(1)(B). See 2015 Amendment note below.

Subsecs. (g)(2)(A), (B)(ii), (i)(5)(B). Pub. L. 115–91, §1081(b)(2), repealed Pub. L. 114–92, §883(f)(1)(A). See 2015 Amendment notes below.

Subsec. (i)(10), (11). Pub. L. 115–91, §912(a)(2), added pars. (10) and (11).

2016—Pub. L. 114–328, §1081(c)(5), added subsec. (f) to section 883 of Pub. L. 114–92. See 2015 Amendment notes below.

Subsec. (d)(1)(B). Pub. L. 114–328, §1081(a)(6)(A), inserted ''to'' before ''eliminate''.

Subsec. (g)(1)(E). Pub. L. 114–328, §1081(a)(6)(B), inserted ''the system'' before ''is in compliance''.

Subsec. (i)(5). Pub. L. 114–328, §1081(a)(6)(C), struck out ''program'' after ''system'' in heading.

2015—Pub. L. 114–92, §883(f)(2), as added by Pub. L. 114–328, §1081(c)(5), repealed second par. (3) of section 901(k) of Pub. L. 113–291. See 2014 Amendment notes below.

Pub. L. 114–92, §883(a)(1), amended section generally. Prior to amendment, section related to architecture, accountability, and modernization of defense business systems.

Subsecs. (c)(2), (e)(1). Pub. L. 114–92, §883(f)(1)(A), as added by Pub. L. 114–328, §1081(c)(5), which directed the substitution of ''Under Secretary of Defense for Business Management and Information'' for ''Deputy Chief Management Officer of the Department of Defense'', was repealed by Pub. L. 115–91, §1081(b)(2).

Subsec. (f)(1). Pub. L. 114–92, §883(f)(1)(B), as added by Pub. L. 114–328, §1081(c)(5), which directed the substitution of ''Under Secretary of Defense for Business Management and Information'' for ''Deputy Chief Management Officer'', was repealed by Pub. L. 115–91, §1081(b)(2).

Subsecs. (g)(2)(A), (B)(ii), (i)(5)(B). Pub. L. 114–92, §883(f)(1)(A), as added by Pub. L. 114–328, §1081(c)(5), which directed the substitution of ''Under Secretary of Defense for Business Management and Information'' for ''Deputy Chief Management Officer of the Department of Defense'', was repealed by Pub. L. 115–91, §1081(b)(2).

Subsec. (j)(5). Pub. L. 114–92, §1081(a)(7), substituted ''section 3552(b)(6)'' for ''section 3552(b)(5)''. Amendment was executed prior to amendment by Pub. L. 114–92, §883(a)(1), see above, pursuant to section 1081(e) of Pub. L. 114–92, set out as a note under section 101 of this title.

2014—Subsec. (a). Pub. L. 113–291, §901(d)(1), inserted ''and'' at end of par. (1), substituted period for ''; and'' at end of par. (2), and struck out par. (3) which read as follows: ''the certification of the investment review board under paragraph (2) has been approved by the Defense Business Systems Management Committee established by section 186 of this title.''

Subsec. (a)(1)(A). Pub. L. 113–291, §803(b)(1), inserted '', including business process mapping,'' after ''re-engineering efforts''.

Subsec. (c)(1). Pub. L. 113–291, §901(d)(2), substituted ''investment review board established under subsection (g)'' for ''Defense Business Systems Management Committee'' in introductory provisions.

Subsecs. (c)(2)(E), (f)(1)(D), (E), (2)(E). Pub. L. 113–291, §901(k)(3), which directed substitution of ''the Under Secretary of Defense for Business Management and Information'' for ''the Deputy Chief Management Officer of the Department of Defense'', but could not be executed following the general amendment of the section by Pub. L. 114–92, was repealed by Pub. L. 114–92, §883(f)(2), as added by Pub. L. 114–328, §1081(c)(5). See 2015 and 2016 Amendment notes above.

Subsec. (g)(1). Pub. L. 113–291, §901(k)(3), which directed substitution of ''the Under Secretary of Defense for Business Management and Information'' for ''the Deputy Chief Management Officer of the Department of Defense'', but could not be executed following the general amendment of the section by Pub. L. 114–92, was repealed by Pub. L. 114–92, §883(f)(2), as added by Pub. L. 114–328, §1081(c)(5). See 2015 and 2016 Amendment notes above.

Pub. L. 113–291, §901(d)(3)(A), struck out '', not later than March 15, 2012,'' before ''to establish an investment review board''.

Subsec. (g)(2)(C). Pub. L. 113–291, §901(d)(3)(B), substituted ''the investment review'' for ''each investment review'' in introductory provisions.

Subsec. (g)(2)(F). Pub. L. 113–291, §901(d)(3)(C), struck out ''and the Defense Business Systems Management Committee, as required by section 186(c) of this title,'' after ''Secretary of Defense''.

Subsec. (g)(3). Pub. L. 113–291, §1071(f)(16), struck out ''(A)'' after ''(3)''.

Subsec. (g)(3)(A). Pub. L. 113–291, §901(k)(3), which directed substitution of ''Under Secretary of Defense for Business Management and Information'' for ''Deputy Chief Management Officer'' the first place appearing, and ''Under Secretary'' for ''Deputy Chief Management Officer'' the second, third, and fourth places appearing, but could not be executed following the general amendment of the section by Pub. L. 114–92, was repealed by Pub. L. 114–92, §883(f)(2), as added by Pub. L. 114–328, §1081(c)(5). See 2015 and 2016 Amendment notes above.

Subsec. (j)(1). Pub. L. 113–291, §803(a), designated existing provisions as subpar. (A), struck out '', other than a national security system,'' after ''information system'', and added subpar. (B).

Subsec. (j)(5). Pub. L. 113–283 substituted ''section 3552(b)(5)'' for ''section 3542(b)(2)''.

Subsec. (j)(6). Pub. L. 113–291, §803(b)(2), added par. (6).

2013—Subsec. (e)(1). Pub. L. 113–66, §901(1), substituted ''target defense business systems computing environment described in subsection (d)(3)'' for ''defense business enterprise architecture''.

Subsec. (e)(2). Pub. L. 113–66, §901(2), substituted ''that will be phased out of the defense business systems computing environment within three years after review and certification as 'legacy systems' by the investment management process established under subsection (g)'' for ''existing as of September 30, 2011 (known as 'legacy systems') that will not be part of the defense business enterprise architecture'' and struck out ''that provides for reducing the use of those legacy systems in phases'' before period at end.

Subsec. (e)(3). Pub. L. 113–66, §901(3), substituted ''existing systems that are part of the target defense business systems computing environment'' for ''legacy systems (referred to in subparagraph (B)) that will be a part of the target defense business systems computing environment described in subsection (d)(3)''.

Subsec. (g)(3). Pub. L. 112–239 added par. (3).

2011—Pub. L. 112–81 amended section generally. Prior to amendment, section related to architecture, accountability, and modernization of defense business systems.

Subsec. (a). Pub. L. 111–383 substituted ''Funds'' for ''Effective October 1, 2005, funds''.

2009—Subsec. (a). Pub. L. 111–84, §1072(a)(1)(A), (B), added par. (1) and redesignated former pars. (1) and (2) as (2) and (3), respectively.

Subsec. (a)(2)(A). Pub. L. 111–84, §1072(a)(1)(C), added subpar. (A) and struck out former subpar. (A), which read as follows: ''is in compliance with the enterprise architecture developed under subsection (c);''.

Subsec. (a)(3). Pub. L. 111–84, §1072(a)(1)(D), substituted ''the certification by the approval authority and the determination by the chief management officer are'' for ''the certification by the approval authority is''.

Subsec. (f). Pub. L. 111–84, §1072(a)(2), designated existing provisions as par. (1), redesignated former pars. (1) to (5) as subpars. (A) to (E), respectively, of par. (1), in subpar. (E) substituted ''subparagraphs (A) through (D)'' for ''paragraphs (1) through (4)'', and added par. (2).

2008—Subsec. (i). Pub. L. 110–417 substituted ''2013'' for ''2009'' in introductory provisions.

2006—Subsec. (j)(6). Pub. L. 109–364 substituted ''in section 3542(b)(2) of title 44'' for ''in section 2315 of this title''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2017 AMENDMENT

Pub. L. 115–91, div. A, title X, § 1081(b)(2), Dec. 12, 2017, 131 Stat. 1597, provided that the amendment made by section 1081(b)(2) is effective as of Nov. 25, 2015.

EFFECTIVE DATE OF 2016 AMENDMENT

Pub. L. 114–328, div. A, title X, § 1081(c), Dec. 23, 2016, 130 Stat. 2419, provided that the amendment made by section 1081(c)(5) is effective as of Nov. 25, 2015, and as if included in Pub. L. 114–92 as enacted.

EFFECTIVE DATE OF 2015 AMENDMENT

Pub. L. 114–92, div. A, title VIII, § 883(f)(1), as added by Pub. L. 114–328, div. A, title X, § 1081(c)(5), Dec. 23, 2016, 130 Stat. 2419, which provided that the amendment made by section 883(f)(1) was effective on the effective date specified in former section 901(a)(1) of Pub. L. 113–291 (Feb. 1, 2017), was repealed by Pub. L. 115–91, div. A, title X, § 1081(b)(2), Dec. 12, 2017, 131 Stat. 1597.

EFFECTIVE DATE OF 2014 AMENDMENT

Pub. L. 113–291, div. A, title IX, § 901(k)(3), Dec. 19, 2014, 128 Stat. 3468, which provided that the amendment made by section 901(k)(3) was effective on the effective date specified in former section 901(a)(1) of Pub. L. 113–291 (Feb. 1, 2017), was repealed by Pub. L. 114–92, div. A, title VIII, § 883(f)(2), as added by Pub. L. 114–328, div. A, title X, § 1081(c)(5), Dec. 23, 2016, 130 Stat. 2420.

TRANSFER OF FUNCTIONS

Position of Chief Management Officer of the Department of Defense effectively abolished upon the repeal of section 132a of this title by Pub. L. 116–283, div. A, title IX, § 901(a)(1), Jan. 1, 2021, 134 Stat. 3794. Duties, personnel, and functions of the Chief Management Officer transferred to other Department of Defense officers, employees, and organizations, and any reference to the Chief Management Officer of the Department of Defense to be deemed to refer to the applicable Department of Defense officer or employee as so designated, see section 901(b), (c) of Pub. L. 116–283, set out in a note under former section 132a of this title.

PILOT PROGRAM ON USE OF ARTIFICIAL INTELLIGENCE FOR CERTAIN WORKFLOW AND OPERATIONS TASKS

Pub. L. 118–159, div. A, title II, § 237, Dec. 23, 2024, 138 Stat. 1842, provided that:

''(a) PILOT PROGRAM REQUIRED.—Beginning not later than 60 days after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Defense shall carry out a pilot program to assess the feasibility and advisability of using artificial intelligence-enabled software to optimize the workflow and operations for—

''(1) depots, shipyards, or other manufacturing facilities run by the Department of Defense; and

''(2) contract administration for the Department, including—

''(A) the adjudication and review of contracts; and

''(B) activities related to the Modernization and Analytics Initiative managed by the Defense Contract Management Agency.

''(b) METHOD OF IMPLEMENTATION.—The Secretary of Defense may carry out subsection (a) through—

''(1) the establishment of a new pilot program; or

''(2) the designation of an existing initiative of the Department of Defense to serve as the pilot program required under such subsection.

''(c) SOFTWARE.—In carrying out the pilot program required by subsection (a), the Secretary shall—

''(1) use best in breed software platforms;

''(2) consider industry best practices in the selection of software programs;

''(3) implement the program based on human centered design practices to best identify the business needs for improvement; and

''(4) demonstrate connection to enterprise platforms of record with authoritative data sources.

''(d) CONSULTATION.—In carrying out the activities described in subsection (a)(1) under the pilot program, the Secretary of Defense shall consult with—

''(1) the Under Secretary of Defense for Acquisition and Sustainment;

''(2) the Secretary of the Army;

''(3) the Secretary of the Navy; and

''(4) the Secretary of the Air Force.

''(e) REPORT.—Not later than one year after the date of the commencement of the pilot program under subsection (a), the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report containing the following information:

''(1) An evaluation of each software platform used in the pilot program.

''(2) An analysis of how workflows and operations were modified as part of the pilot program.

''(3) A quantitative assessment of the impact the software had at each of the locations in which the pilot program was carried out.''

NEXT GENERATION BUSINESS HEALTH METRICS

Pub. L. 118–31, div. A, title IX, § 921, Dec. 22, 2023, 137 Stat. 373, provided that:

''(a) METRICS REQUIRED.—The Secretary of Defense, in coordination with the Secretaries of the military departments, shall develop an updated set of business health metrics to inform decision-making by senior leaders of the Department of Defense.

''(b) ELEMENTS.—In developing the metrics required by subsection (a), the Secretary of Defense shall—

''(1) using the latest literature on performance measurement, determine what additional new metrics should be implemented, or current metrics should be adapted, to reduce output-based measures and emphasize objective, measurable indicators aligned to enduring strategic goals of the Department of Defense;

''(2) assess the current business processes of the Department and provide recommendations to align the metrics with available data sources to determine what gaps might exist in such processes;

''(3) ensure that data can be collected automatically and, on a long-term basis, in a manner that provides for longitudinal analysis;

''(4) link the metrics with the Strategic Management Plan and other performance documents guiding the Department;

''(5) identify any shortfalls in resources, data, training, policy, or law that could be an impediment to implementing the metrics;

''(6) revise leading and lagging indicators associated with each such metric to provide a benchmark against which to assess progress;

''(7) improve visualization of and comprehension for the use of the metrics in data-driven decision-making, including adoption of new policies and training as needed;

''(8) incorporate the ability to aggregate and disaggregate data to provide the ability to focus on functional, component-level metrics; and

''(9) increase standardization of the use and collection of business health metrics across the Department.

''(c) ADDITIONAL SUPPORT.—The Secretary of Defense may enter into a contract or other agreement with a federally funded research and development center or university-affiliated research center to support the development of the metrics required under subsection (a).''

PRIZE COMPETITIONS FOR BUSINESS SYSTEMS MODERNIZATION

Pub. L. 118–31, div. A, title XV, §1525, Dec. 22, 2023, 137 Stat. 556, provided that:

''(a) ESTABLISHMENT.—Not later than 270 days after the date of the enactment of this Act [Dec. 22, 2023], under the authority of section 4025 of title 10, United States Code, the Secretary of Defense shall establish one or more prize competitions to support the business systems modernization goals of the Department of Defense.

''(b) SCOPE.—

''(1) IN GENERAL.—The Secretary of Defense shall structure any prize competition established under subsection (a) to complement, and to the extent practicable, accelerate the delivery or expand the functionality of business systems capabilities sought by the Secretaries of the military departments that are in operation, in development, or belong to any broad class of systems covered by the defense business enterprise architecture specified in section 2222(e) of title 10, United States Code.

''(2) AREAS FOR CONSIDERATION.—In carrying out subsection (a), the Secretary of Defense and the Secretaries of the military departments shall consider the following:

''(A) Integration of artificial intelligence or machine learning capabilities.

''(B) Data analytics, business intelligence, or related visualization capabilities.

''(C) Automated updating of business architectures, business systems integration, or documentation relating to existing systems or manuals.

''(D) Improvements to interfaces or processes for interacting with other non-Department of Defense business systems.

''(E) Updates or replacements for legacy defense business systems to improve operational effectiveness and efficiency, such as the system of the Defense Logistics Agency known as the 'Mechanization of Contract Administration Services' system, or any successor system.

''(F) Contract writing systems, or expanded capabilities relating to such systems, that may be integrated into existing systems of the Department of Defense.

''(G) Pay and personnel systems, or expanded capabilities relating to such systems, that may be integrated into existing systems of the Department of Defense.

''(H) Other finance and accounting systems, or expanded capabilities relating to such systems, that may be integrated into existing systems of the Department of Defense.

''(I) Systems supporting the defense industrial base and related supply chain visibility, analytics, and management.

''(c) FRAMEWORK.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the framework to be used in carrying out the prize competition under subsection (a).

''(d) ANNUAL BRIEFINGS.—Not later than October 1 of each year until the date of termination under subsection (e), the Secretary of Defense shall provide to the congressional defense committees a briefing on the results of the prize competition under subsection (a).

''(e) TERMINATION.—The authority to carry out the prize competition under subsection (a) shall terminate on September 30, 2028.''

IMPROVED RECORDING AND MAINTAINING OF DEPARTMENT OF DEFENSE REAL PROPERTY DATA

Pub. L. 116–92, div. B, title XXVIII, §2823, Dec. 20, 2019, 133 Stat. 1889, provided that:

''(a) INITIAL REPORT.—Not later than 150 days after the date of the enactment of this Act [Dec. 20, 2019], the Undersecretary [probably should be ''Under Secretary''] of Defense for Acquisition and Sustainment shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that evaluates service-level best practices for recording and maintaining real property data.

''(b) ISSUANCE OF GUIDANCE.—Not later than 300 days after the date of the enactment of this Act, the Undersecretary [probably should be ''Under Secretary''] of Defense for Acquisition and Sustainment shall issue service-wide guidance on the recording and collection of real property data based on the best practices described in the report.''

REFORM OF BUSINESS ENTERPRISE OPERATIONS IN SUPPORT OF CERTAIN ACTIVITIES ACROSS DEPARTMENT OF DEFENSE

Pub. L. 115–232, div. A, title IX, §921(b), Aug. 13, 2018, 132 Stat. 1927, provided that:

''(1) PERIODIC REFORM.—

''(A) IN GENERAL.—Not later than January 1, 2020, and not less frequently than once every five years thereafter, the Secretary of Defense shall, acting through the Chief Management Officer of the Department of Defense, reform enterprise business operations of the Department of Defense, through reductions, eliminations, or improvements, across all organizations and elements of the Department with respect to covered activities in order to increase effectiveness and efficiency of mission execution.

''(B) CMO REPORTS.—Not later than January 1 of every fifth calendar year beginning with January 1, 2025, the Chief Management Officer shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that describes the activities carried out by the Chief Management Officer under this subsection during the preceding five years, including an estimate of any cost savings achieved as a result of such activities.

''(2) COVERED ACTIVITIES DEFINED.—In this subsection, the term 'covered activities' means any activity relating to civilian resources management, logistics management, services contracting, or real estate management.

''(3) REPORTING FRAMEWORK.—Not later than January 1, 2020, the Chief Management Officer shall establish a consistent reporting framework to establish a baseline for the costs to perform all covered activities, and shall submit to Congress a report that, for each individual covered activity performed in fiscal year 2019, identifies the following:

''(A) The component or components of the Department responsible for performing such activity, and a business process map of such activity, in fiscal year 2019.

''(B) The number of the military, civilian, and contractor personnel of the component or components of the Department who performed such activity in that fiscal year.

''(C) The manpower requirements for such activity as of that fiscal year.

''(D) The systems and other resources associated with such activity as of that fiscal year.

''(E) The cost in dollars of performing such activity in fiscal year 2019.

''(4) INITIAL PLAN.—Not later than February 1, 2019, the Chief Management Officer shall submit to the congressional defense committees a plan, schedule, and cost estimate for conducting the reforms required under paragraph (1)(A).

''(5) CERTIFICATION OF COST SAVINGS.—Not later than January 1, 2020, the Chief Management Officer shall certify to the congressional defense committees that the savings and costs incurred as a result of activities carried out under paragraph (1) will achieve savings in fiscal year 2020 against the total amount obligated and expended for covered activities in fiscal year 2019 of—

''(A) not less than 25 percent of the cost in dollars of performing covered activities in fiscal year 2019 as specified pursuant to paragraph (3)(E); or

''(B) if the Chief Management Officer determines that achievement of savings of 25 percent or more will create overall inefficiencies for the Department, notice and justification will be submitted to the congressional defense committees specifying a lesser percentage of savings that the Chief Management Officer determines to be necessary to achieve efficiencies in the delivery of covered activities, which notice and justification shall be submitted by not later than October 1, 2019, together with a description of the efficiencies to be achieved.

''(6) COMPTROLLER GENERAL REPORTS.—The Comptroller General of the United States shall submit to the congressional defense committees the following:

''(A) Not later than 90 days after the submittal of the plan under paragraph (4), a report that verifies whether the plan is feasible.

''(B) Not later than 270 days after the date of enactment of this Act [Aug. 13, 2018], a report setting forth an assessment of the actions taken under paragraph (1)(A) since the date of the enactment of this Act.

''(C) Not later than 270 days after the submittal of the reporting framework under paragraph (3), a report that verifies whether the baseline established in the framework is accurate.

''(D) Not later than 270 days after the submittal of the report under paragraph (5), a report that verifies—

''(i) whether the activities described in the report were carried out; and

''(ii) whether any cost savings estimated in the report are accurate.''

[For abolition and transfer of functions of Chief Management Officer of the Department of Defense, see Transfer of Functions note above.]

ANALYSIS OF DEPARTMENT OF DEFENSE BUSINESS MANAGEMENT AND OPERATIONS DATASETS TO PROMOTE SAVINGS AND EFFICIENCIES

Pub. L. 115–232, div. A, title IX, §922, Aug. 13, 2018, 132 Stat. 1929, provided that:

''(a) IN GENERAL.—The Chief Management Officer of the Department of Defense shall develop a policy on analysis of Department of Defense datasets on business management and business operations by the public for purposes of accessing data analysis capabilities that would promote savings and efficiencies and otherwise enhance the utility of such datasets to the Department.

''(b) INITIAL DISCHARGE OF POLICY.—

''(1) IN GENERAL.—The Chief Management Officer shall commence the discharge of the policy required pursuant to subsection (a) by—

''(A) identifying one or more matters—

''(i) that are of significance to the Department of Defense;

''(ii) that are currently unresolved; and

''(iii) whose resolution from a business management or business operations dataset of the Department could benefit from a method or technique of analysis not currently familiar to the Department;

''(B) identifying between three and five business management or business operations datasets of the Department not currently available to the public whose evaluation could result in novel data analysis solutions toward management or operations problems of the Department identified by the Chief Management Officer; and

''(C) encouraging, whether by competition or other mechanisms, the evaluation of the datasets described in subparagraph (B) by appropriate persons and entities in the public or private sector (including academia).

''(2) PROTECTION OF SECURITY AND CONFIDENTIALITY.—In providing for the evaluation of datasets pursuant to this subsection, the Chief Management Officer shall take appropriate actions to protect the security and confidentiality of any information contained in the datasets, including through special precautions to ensure that any personally identifiable information is not included and no release of information will adversely affect national security missions.''

[For abolition and transfer of functions of Chief Management Officer of the Department of Defense, see Transfer of Functions note above.]

AUDIT OF FINANCIAL SYSTEMS OF THE DEPARTMENT OF DEFENSE BY PROFESSIONAL ACCOUNTANTS

Pub. L. 115–232, div. A, title X, §1004, Aug. 13, 2018, 132 Stat. 1947, provided that: ''The Secretary of Defense, acting through the Under Secretary of Defense (Comptroller) or an appropriate official of a military department, shall ensure that each major implementation of, or modification to, a business system that contributes to financial information of the Department of Defense is reviewed by professional accountants with experience reviewing Federal financial systems to validate that such financial system will meet any applicable Federal requirements. The Secretary of Defense shall ensure that such accountants—

''(1) are provided all necessary data and records; and

''(2) report independently on their findings.''

STANDARDIZED BUSINESS PROCESS RULES FOR MILITARY INTELLIGENCE PROGRAM

Pub. L. 115–232, div. A, title XVI, §1624(a), Aug. 13, 2018, 132 Stat. 2119, provided that:

''(1) DEVELOPMENT.—Not later than October 1, 2020, the Chief Management Officer of the Department of Defense, in coordination with the Under Secretary of Defense (Comptroller) and the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security], shall develop and implement standardized business process rules for the planning, programming, budgeting, and execution process for the Military Intelligence Program.

''(2) TREATMENT OF DATA.—The Chief Management Officer shall develop the standardized business process rules under paragraph (1) in accordance with section 911 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 131 Stat. 1519; 10 U.S.C. 2222 note) [set out below] and section 2222(e)(6) of title 10, United States Code.

''(3) USE OF EXISTING SYSTEMS.—In developing the standardized business process rules under paragraph (1), to the extent practicable, the Chief Management Officer shall use enterprise business systems of the Department of Defense in existence as of the date of the enactment of this Act [Aug. 13, 2018].

''(4) REPORT.—Not later than March 1, 2019, the Chief Management Officer of the Department of Defense, the Under Secretary of Defense (Comptroller), and the Under Secretary of Defense for Intelligence shall jointly submit to the appropriate congressional committees a report containing a plan to develop the standardized business process rules under paragraph (1).

''(5) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this subsection, the term 'appropriate congressional committees' means the following:

''(A) The congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives].

''(B) The Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.''

POLICY ON TREATMENT OF DEFENSE BUSINESS SYSTEM DATA RELATED TO BUSINESS OPERATIONS AND MANAGEMENT

Pub. L. 115–91, div. A, title IX, §911, Dec. 12, 2017, 131 Stat. 1519, provided that:

''(a) ESTABLISHMENT OF POLICY.—Not later than one year after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall establish a data policy for the Department of Defense that mandates that any data contained in a defense business system related to business operations and management is an asset of the Department of Defense.

''(b) AVAILABILITY.—As part of the policy required by subsection (a), the Secretary of Defense shall ensure that, except as otherwise provided by law or regulation, data described in such subsection shall be made readily available to members of the Office of the Secretary of Defense, the Joint Staff, the military departments, the combatant commands, the Defense Agencies, the Department of Defense Field Activities, and all other offices, agencies, activities, and commands of the Department of Defense, as applicable.''

ESTABLISHMENT OF DATA ANALYTICS CAPABILITY

Pub. L. 115–91, div. A, title IX, §912(e), Dec. 12, 2017, 131 Stat. 1521, provided that:

''(1) DATA ANALYTICS CAPABILITY REQUIRED.—Not later than September 30, 2020, the Chief Management Officer of the Department of Defense shall establish and maintain within the Department of Defense a data analytics capability for purposes of supporting enhanced oversight and management of the Defense Agencies and Department of Defense Field Activities.

''(2) ELEMENTS.—The data analytics capability shall permit the following:

''(A) The maintenance on a continuing basis of an accurate tabulation of the amounts expended by the Defense Agencies and Department of Defense Field Activities on Government and contractor personnel.

''(B) The maintenance on a continuing basis of an accurate number of the personnel currently supporting the Defense Agencies and Department of Defense Field Activities, including the following:

''(i) Members of the regular components of the Armed Forces.

''(ii) Members of the reserve components of the Armed Forces.

''(iii) Civilian employees of the Department of Defense.

''(iv) Detailees, whether from another organization or element of the Department or from another department or agency of the Federal Government.

''(C) The tracking of costs for employing contract personnel, including federally funded research and development centers.

''(D) The maintenance on a continuing basis of the following:

''(i) An identification of the functions being performed by each Defense Agency and Department of Defense Field Activity.

''(ii) An accurate tabulation of the amounts being expended by each Defense Agency and Department of Defense Field Activity on its functions.

''(3) REPORTING REQUIREMENTS.—

''(A) INTERIM REPORT.—Not later than one year after the date of the enactment of this Act [Dec. 12, 2017], the Chief Management Officer of the Department of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on progress in establishing the data analytics capability. The report shall include the following:

''(i) A description and assessment of the efforts of the Chief Management Officer through the date of the report to establish the data analytics capability.

''(ii) A description of current gaps in the data required to establish the data analytics capability, and a description of the efforts to be undertaken to eliminate such gaps.

''(B) FINAL REPORT.—Not later than December 31, 2020, the Chief Management Officer shall submit to the congressional defense committees a report on the data analytics capability as established pursuant to this section.''

DATA INTEGRATION STRATEGIES PILOT PROGRAMS

Pub. L. 115–91, div. A, title IX, §912(f), Dec. 12, 2017, 131 Stat. 1522, provided that:

''(1) IN GENERAL.—The Secretary of Defense shall carry out pilot programs to develop data integration strategies for the Department of Defense to address high-priority management challenges of the Department.

''(2) ELEMENTS.—The pilot programs carried out under the authority of this subsection shall involve data integration strategies to address challenges of the Department with respect to the following:

''(A) The budget of the Department.

''(B) Logistics.

''(C) Personnel security and insider threats.

''(D) At least two other high-priority challenges of the Department identified by the Secretary for purposes of this subsection.

''(3) REPORT ON PILOT PROGRAMS.—Not later than one year after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report describing the pilot programs to be carried out under this section, including the challenge of the Department to be addressed by the pilot program and the manner in which the data integration strategy under the pilot program will address the challenge. If any proposed pilot program requires legislative action for the waiver or modification of a statutory requirement that otherwise prevents or impedes the implementation of the pilot program, the Secretary shall include in the report a recommendation for legislative action to waive or modify the statutory requirement.''

IMPROPER PAYMENT MATTERS

Pub. L. 115–91, div. A, title X, §1003, Dec. 12, 2017, 131 Stat. 1542, provided that: ''Subject to the authority, direction, and control of the Secretary of Defense, the Under Secretary of Defense (Comptroller) shall take the following actions:

''(1) With regard to estimating improper payments:

''(A) Establish and implement key quality assurance procedures, such as reconciliations, to ensure the completeness and accuracy of sampled populations.

''(B) Revise the procedures for the sampling methodologies of the Department of Defense so that such procedures—

''(i) comply with Office of Management and Budget guidance and generally accepted statistical standards;

''(ii) produce statistically valid improper payment error rates, statistically valid improper payment dollar estimates, and appropriate confidence intervals for both; and

''(iii) in meeting clauses (i) and (ii), take into account the size and complexity of the transactions being sampled.

''(2) With regard to identifying programs susceptible to significant improper payments, conduct a risk assessment that complies with the Improper Payments Elimination and Recovery Act of 2010 (Public Law 111–204 [See Short Title of 2010 Amendment note set out under section 3301 of Title 31, Money and Finance]) and the amendments made by that Act (in this section collectively referred to as 'IPERA').

''(3) With regard to reducing improper payments, establish procedures that produce corrective action plans that—

''(A) comply fully with IPERA and associated Office of Management and Budget guidance, including by holding individuals responsible for implementing corrective actions and monitoring the status of corrective actions; and

''(B) are in accordance with best practices, such as those recommended by the Chief Financial Officers Council, including by providing for—

''(i) measurement of the progress made toward remediating root causes of improper payments; and

''(ii) communication to the Secretary of Defense and the heads of departments, agencies, and

organizations and elements of the Department of Defense, and key stakeholders, on the progress made toward remediating the root causes of improper payments.

''(4) With regard to implementing recovery audits for improper payments, develop and implement procedures to—

''(A) identify costs related to the recovery audits and recovery efforts of the Department of Defense; and

''(B) evaluate improper payment recovery efforts in order to ensure that they are cost effective.

''(5) Monitor the implementation of the revised chapter of the Financial Management Regulations on recovery audits in order to ensure that the Department of Defense, the military departments, the Defense Agencies, and the other organizations and elements of the Department of Defense either conduct recovery audits or demonstrate that it is not cost effective to do so.

''(6) Develop and submit to the Office of Management and Budget for approval a payment recapture audit plan that fully complies with Office of Management and Budget guidance.

''(7) With regard to reporting on improper payments, design and implement procedures to ensure that the annual improper payment and recovery audit reporting of the Department of Defense is complete, accurate, and complies with IPERA and associated Office of Management and Budget guidance.''

FINANCIAL OPERATIONS DASHBOARD FOR THE DEPARTMENT OF DEFENSE

Pub. L. 115–91, div. A, title X, §1005, Dec. 12, 2017, 131 Stat. 1544, provided that:

''(a) IN GENERAL.—The Under Secretary of Defense (Comptroller) shall develop and maintain on an Internet website available to Department of Defense agencies a tool (commonly referred to as a 'dashboard)' [sic] to permit officials to track key indicators of the financial performance of the Department of Defense. Such key indicators may include outstanding accounts payable, abnormal accounts payable, outstanding advances, unmatched disbursements, abnormal undelivered orders, negative unliquidated obligations, violations of sections 1341 and 1517(a) of title 31, United States Code (commonly referred to as the 'Anti-Deficiency Act'), costs deriving from payment delays, interest penalty payments, and improper payments, and actual savings realized through interest payments made, discounts for timely or advanced payments, and other financial management and improvement initiatives.

''(b) INFORMATION COVERED.—The tool shall cover financial performance information for the military departments, the defense agencies, and any other organizations or elements of the Department of Defense.

''(c) TRACKING OF PERFORMANCE OVER TIME.—The tool shall permit the tracking of financial performance over time, including by month, quarter, and year, and permit users of the tool to export both current and historical data on financial performance.

''(d) UPDATES.—The information covered by the tool shall be updated not less frequently than quarterly.''

IMPROVED MANAGEMENT PRACTICES TO REDUCE COST AND IMPROVE PERFORMANCE OF CERTAIN DEPARTMENT OF DEFENSE ORGANIZATIONS

Pub. L. 114–328, div. A, title VIII, §894, Dec. 23, 2016, 130 Stat. 2325, provided that:

''(a) IN GENERAL.—Beginning not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary of Defense shall designate units, subunits, or entities of the Department of Defense, other than Centers of Industrial and Technical Excellence designated pursuant to section 2474 of title 10, United States Code, that conduct work that is commercial in nature or is not inherently governmental to prioritize efforts to conduct business operations in a manner that uses modern, commercial management practices and principles to reduce the costs and improve the performance of such organizations.

''(b) ADOPTION OF MODERN BUSINESS PRACTICES.—The Secretary shall ensure that each such unit, subunit, or entity of the Department described in subsection (a) is authorized to adopt and implement best commercial and business management practices to achieve the goals described in such subsection.

''(c) WAIVERS.—The Secretary shall authorize waivers of Department of Defense, military service, and Defense Agency regulations, as appropriate, to achieve the goals in subsection (a), including in the following areas:

''(1) Financial management.

''(2) Human resources.

''(3) Facility and plant management.

''(4) Acquisition and contracting.

''(5) Partnerships with the private sector.

''(6) Other business and management areas as identified by the Secretary.

''(d) GOALS.—The Secretary of Defense shall identify savings goals to be achieved through the implementation of the commercial and business management practices adopted under subsection (b), and establish a schedule for achieving the savings.

''(e) BUDGET ADJUSTMENT.—The Secretary shall establish policies to adjust organizational budget allocations, at the Secretary's discretion, for purposes of—

''(1) using savings derived from implementation of best commercial and business management practices for high priority military missions of the Department of Defense;

''(2) creating incentives for the most efficient and effective development and adoption of new commercial and business management practices by organizations; and

''(3) investing in the development of new commercial and business management practices that will result in further savings to the Department of Defense.

''(f) BUDGET BASELINES.—Beginning not later than one year after the date of the enactment of this Act [Dec. 23, 2016], each such unit, subunit, or entity of the Department described in subsection (a) shall, in accordance with such guidance as the Secretary of Defense shall establish for purposes of this section—

''(1) establish an annual baseline cost estimate of its operations; and

''(2) certify that costs estimated pursuant to paragraph (1) are wholly accounted for and presented in a format that is comparable to the format for the presentation of such costs for other elements of the Department or consistent with best commercial practices.''

INCREASED USE OF COMMERCIAL DATA INTEGRATION AND ANALYSIS PRODUCTS FOR THE PURPOSE OF PREPARING FINANCIAL STATEMENT AUDITS

Pub. L. 114–328, div. A, title X, §1003, Dec. 23, 2016, 130 Stat. 2380, which required the Secretary of Defense to procure or develop technologies or services to improve data collection and analyses to support preparation of auditable financial statements for the Department of Defense, was repealed by Pub. L. 115–91, div. A, title X, §1002(f)(3), Dec. 12, 2017, 131 Stat. 1542. See section 240e of this title.

SCIENCE AND TECHNOLOGY ACTIVITIES TO SUPPORT BUSINESS SYSTEMS INFORMATION TECHNOLOGY ACQUISITION PROGRAMS

Pub. L. 114–92, div. A, title II, §217, Nov. 25, 2015, 129 Stat. 770, as amended by Pub. L. 115–232, div. A, title X, §1081(f)(1)(A)(v), Aug. 13, 2018, 132 Stat. 1986; Pub. L. 116–92, div. A, title IX, §902(26), Dec. 20, 2019, 133 Stat. 1545; Pub. L. 116–283, div. A, title XVIII, §1806(e)(3)(B), Jan. 1, 2021, 134 Stat. 4156, provided that:

''(a) IN GENERAL.—The Secretary of Defense, acting through the Under Secretary of Defense for Acquisition and Sustainment and Under Secretary of Defense for

Research and Engineering, the Chief Management Officer, and the Chief Information Officer, shall establish a set of science, technology, and innovation activities to improve the acquisition outcomes of major automated information systems through improved performance and reduced developmental and life cycle costs.

''(b) EXECUTION OF ACTIVITIES.—The activities established under subsection (a) shall be carried out by such military departments and Defense Agencies as the Under Secretary and the Chief Management Officer consider appropriate.

''(c) ACTIVITIES.—

''(1) IN GENERAL.—The set of activities established under subsection (a) may include the following:

''(A) Development of capabilities in Department of Defense laboratories, test centers, and federally funded research and development centers to provide technical support for acquisition program management and business process re-engineering activities.

''(B) Funding of intramural and extramural research and development activities as described in subsection (e).

''(2) CURRENT ACTIVITIES.—The Secretary shall identify the current activities described in subparagraphs (A) and (B) of paragraph (1) that are being carried out as of the date of the enactment of this Act [Nov. 25, 2015]. The Secretary shall consider such current activities in determining the set of activities to establish pursuant to subsection (a).

''(d) GAP ANALYSIS.—In establishing the set of activities under subsection (a), not later than 270 days after the date of the enactment of this Act [Nov. 25, 2015], the Secretary, in coordination with the Secretaries of the military departments and the heads of the Defense Agencies, shall conduct a gap analysis to identify activities that are not, as of such date, being pursued in the current science and technology program of the Department. The Secretary shall use such analysis in determining—

''(1) the set of activities to establish pursuant to subsection (a) that carry out the purposes specified in subsection (c)(1); and

''(2) the proposed funding requirements and timelines.

''(e) FUNDING OF INTRAMURAL AND EXTRAMURAL RESEARCH AND DEVELOPMENT.—

''(1) IN GENERAL.—In carrying out the set of activities required by subsection (a), the Secretary may award grants or contracts to eligible entities to carry out intramural or extramural research and development in areas of interest described in paragraph (3).

''(2) ELIGIBLE ENTITIES.—For purposes of this subsection, an eligible entity includes the following:

''(A) Entities in the defense industry.

''(B) Institutions of higher education.

''(C) Small businesses.

''(D) Nontraditional defense contractors (as defined in section 3014 of title 10, United States Code).

''(E) Federally funded research and development centers, primarily for the purpose of improving technical expertise to support acquisition efforts.

''(F) Nonprofit research institutions.

''(G) Government laboratories and test centers, primarily for the purpose of improving technical expertise to support acquisition efforts.

''(3) AREAS OF INTEREST.—The areas of interest described in this paragraph are the following:

''(A) Management innovation, including personnel and financial management policy innovation.

''(B) Business process re-engineering.

''(C) Systems engineering of information technology business systems.

''(D) Cloud computing to support business systems and business processes.

''(E) Software development, including systems and techniques to limit unique interfaces and simplify processes to customize commercial software to meet the needs of the Department of Defense.

''(F) Hardware development, including systems and techniques to limit unique interfaces and simplify processes to customize commercial hardware to meet the needs of the Department of Defense.

''(G) Development of methodologies and tools to support development and operational test of large and complex business systems.

''(H) Analysis tools to allow decision-makers to make tradeoffs between requirements, costs, technical risks, and schedule in major automated information system acquisition programs.

''(I) Information security in major automated information system systems.

''(J) Innovative acquisition policies and practices to streamline acquisition of information technology systems.

''(K) Such other areas as the Secretary considers appropriate.

''(f) PRIORITIES.—

''(1) IN GENERAL.—In carrying out the set of activities required by subsection (a), the Secretary shall give priority to—

''(A) projects that—

''(i) address the innovation and technology needs of the Department of Defense; and

''(ii) support activities of initiatives, programs, and offices identified by the Under Secretary and Chief Management Officer; and

''(B) the projects and programs identified in paragraph (2).

''(2) PROJECTS AND PROGRAMS IDENTIFIED.—The projects and programs identified in this paragraph are the following:

''(A) Major automated information system programs.

''(B) Projects and programs under the oversight of the Chief Management Officer.

''(C) Projects and programs relating to defense procurement acquisition policy.

''(D) Projects and programs of the agencies and field activities of the Office of the Secretary of Defense that support business missions such as finance, human resources, security, management, logistics, and contract management.

''(E) Military and civilian personnel policy development for information technology workforce.''

[For abolition and transfer of functions of Chief Management Officer of the Department of Defense, see Transfer of Functions note above.]

DEADLINE FOR GUIDANCE ON COVERED DEFENSE BUSINESS SYSTEMS

Pub. L. 114–92, div. A, title VIII, §883(b), Nov. 25, 2015, 129 Stat. 947, provided that: ''The guidance required by subsection (c)(1) of section 2222 of title 10, United States Code, as amended by subsection (a)(1), shall be issued not later than December 31, 2016.''

COMPTROLLER GENERAL ASSESSMENT REQUIREMENT

Pub. L. 114–92, div. A, title VIII, §883(d)(1), Nov. 25, 2015, 129 Stat. 947, which required the Comptroller General, in odd-numbered years, to submit an assessment of the extent to which the actions taken by the Department of Defense complied with the requirements of this section, was repealed by Pub. L. 115–232, div. A, title VIII, §833(c), Aug. 13, 2018, 132 Stat. 1859, effective Jan. 1, 2020.

ACCOUNTING STANDARDS TO VALUE CERTAIN PROPERTY, PLANT, AND EQUIPMENT ITEMS

Pub. L. 114–92, div. A, title X, §1002, Nov. 25, 2015, 129 Stat. 960, provided that:

''(a) REQUIREMENT FOR CERTAIN ACCOUNTING STANDARDS.—The Secretary of Defense shall work in coordination with the Federal Accounting Standards Advisory Board to establish accounting standards to value large and unordinary general property, plant, and equipment items.

''(b) DEADLINE.—The accounting standards required by subsection (a) shall be established by not later than

September 30, 2017, and be available for use for the full audit on the financial statements of the Department of Defense for fiscal year 2018, as required by section 1003(a) of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 127 Stat. 842; 10 U.S.C. 2222 note).''

ANNUAL AUDIT OF FINANCIAL STATEMENTS OF DEPARTMENT OF DEFENSE COMPONENTS BY INDEPENDENT EXTERNAL AUDITORS

Pub. L. 114–92, div. A, title X, § 1005, Nov. 25, 2015, 129 Stat. 961, which required an annual audit of financial statements of Department of Defense components by independent external auditors, was repealed by Pub. L. 115–91, div. A, title X, § 1002(e)(4), Dec. 12, 2017, 131 Stat. 1541. See section 240d of this title.

DEADLINE FOR ESTABLISHMENT OF INVESTMENT REVIEW BOARD AND INVESTMENT MANAGEMENT PROCESS

Pub. L. 113–291, div. A, title IX, § 901(e), Dec. 19, 2014, 128 Stat. 3464, provided that: ''The investment review board and investment management process required by [former] section 2222(g) of title 10, United States Code, as amended by subsection (d)(3), shall be established not later than March 15, 2015.''

AUDIT OF DEPARTMENT OF DEFENSE FISCAL YEAR 2018 FINANCIAL STATEMENTS

Pub. L. 113–66, div. A, title X, § 1003(a), Dec. 26, 2013, 127 Stat. 842, which required a full audit of the financial statements of the Department of Defense for fiscal year 2018, was repealed by Pub. L. 115–91, div. A, title X, § 1002(b)(2), Dec. 12, 2017, 131 Stat. 1538. For similar provisions requiring annual audits, see section 240a of this title.

REVIEW OF OBLIGATION AND EXPENDITURE THRESHOLDS

Pub. L. 111–383, div. A, title VIII, § 882, Jan. 7, 2011, 124 Stat. 4308, as amended by Pub. L. 113–291, div. A, title IX, § 901(n)(1), Dec. 19, 2014, 128 Stat. 3469; Pub. L. 115–91, div. A, title X, § 1081(b)(1)(D), Dec. 12, 2017, 131 Stat. 1597; Pub. L. 116–92, div. A, title IX, § 902(27), Dec. 20, 2019, 133 Stat. 1546, provided that:

''(a) PROCESS REVIEW.—Not later than one year after the date of the enactment of this Act [Jan. 7, 2011], the Chief Management Officer of the Department of Defense, in coordination with the Chief Management Officer of each military department, the Director of the Office of Performance Assessment and Root Cause Analysis, the Under Secretary of Defense (Comptroller), and the Comptrollers of the military departments, shall complete a comprehensive review of the use and value of obligation and expenditure benchmarks and propose new benchmarks or processes for tracking financial performance, including, as appropriate—

''(1) increased reliance on individual obligation and expenditure plans for measuring program financial performance;

''(2) mechanisms to improve funding stability and to increase the predictability of the release of funding for obligation and expenditure; and

''(3) streamlined mechanisms for a program manager to submit an appeal for funding changes and to have such appeal evaluated promptly.

''(b) TRAINING.—The Under Secretary of Defense for Acquisition and Sustainment and the Under Secretary of Defense (Comptroller) shall ensure that, as part of the training required for program managers and business managers, an emphasis is placed on obligating and expending appropriated funds in a manner that achieves the best value for the Government and that the purpose and limitations of obligation and expenditure benchmarks are made clear.

''(c) REPORT.—The Deputy Chief Management Officer of the Department of Defense shall include a report on the results of the review under this section in the next update of the strategic management plan transmitted to the Committees on Armed Services of the Senate and the House of Representatives under section 904(d) of the National Defense Authorization Act for Fiscal Year 2008 (Public Law 110–181; 122 Stat. 275; 10 U.S.C. note prec. 2201) after the completion of the review.''

[Pub. L. 113–291, div. A, title IX, § 901(n)(1), Dec. 19, 2014, 128 Stat. 3469, formerly set out as a References note under section 131 of this title, which provided that, effective after Feb. 1, 2017, any reference to the Deputy Chief Management Officer of the Department of Defense was to be deemed to refer to the Under Secretary of Defense for Business Management and Information, was repealed by Pub. L. 115–91, div. A, title X, § 1081(b)(1)(D), Dec. 12, 2017, 131 Stat. 1597, effective as of Dec. 23, 2016.]

AUDIT READINESS OF FINANCIAL STATEMENTS OF THE DEPARTMENT OF DEFENSE

Pub. L. 112–239, div. A, title X, § 1005(b), Jan. 2, 2013, 126 Stat. 1904, provided that:

''(1) IN GENERAL.—The Chief Management Officer of the Department of Defense and the Chief Management Officers of each of the military departments shall ensure that plans to achieve an auditable statement of budgetary resources of the Department of Defense by September 30, 2014, include appropriate steps to minimize one-time fixes and manual work-arounds, are sustainable and affordable, and will not delay full auditability of financial statements.

''(2) ADDITIONAL ELEMENTS IN FIAR PLAN REPORT.—Each semi-annual report on the Financial Improvement and Audit Readiness Plan of the Department of Defense submitted by the Under Secretary of Defense (Comptroller) under section 1003(b) of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note) during the period beginning on the date of the enactment of this Act [Jan. 2, 2013] and ending on September 30, 2014, shall include the following:

''(A) A description of the actions taken by the military departments pursuant to paragraph (1).

''(B) A determination by the Chief Management Officer of each military department whether or not such military department is able to achieve an auditable statement of budgetary resources by September 30, 2014, without an unaffordable or unsustainable level of one-time fixes and manual work-arounds and without delaying the full auditability of the financial statements of such military department.

''(C) If the Chief Management Officer of a military department determines under subparagraph (B) that the military department is not able to achieve an auditable statement of budgetary resources by September 30, 2014, as described in that subparagraph—

''(i) an explanation why the military department is unable to meet the deadline;

''(ii) an alternative deadline by which the military department will achieve an auditable statement of budgetary resources; and

''(iii) a description of the plan of the military department for meeting the alternative deadline.''

Pub. L. 112–81, div. A, title X, § 1003, Dec. 31, 2011, 125 Stat. 1555, as amended by Pub. L. 113–291, div. A, title IX, § 901(n)(1), Dec. 19, 2014, 128 Stat. 3469; Pub. L. 115–91, div. A, title X, § 1081(b)(1)(D), Dec. 12, 2017, 131 Stat. 1597, provided that:

''(a) PLANNING REQUIREMENT.—

''(1) IN GENERAL.—The report to be issued pursuant to section 1003(b) of the National Defense Authorization Act for 2010 (Public Law 111–84; 123 Stat. 2440; 10 U.S.C. 2222 note) and provided by not later than May 15, 2012, shall include a plan, including interim objectives and a schedule of milestones for each military department and for the defense agencies, to support the goal established by the Secretary of Defense that the statement of budgetary resources is validated for audit by not later than September 30, 2014. Consistent with the requirements of such section, the plan shall include process and control improvements and business systems modernization efforts necessary for the Department of Defense to consistently prepare time-

ly, reliable, and complete financial management information.

''(2) SEMIANNUAL UPDATES.—The reports to be issued pursuant to such section after the report described in paragraph (1) shall update the plan required by such paragraph and explain how the Department has progressed toward meeting the milestones established in the plan.

''(b) INCLUSION OF SUBORDINATE ACTIVITIES FOR INTERIM MILESTONES.—For each interim milestone established pursuant to section 881 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4306; 10 U.S.C. 2222 note), the Under Secretary of Defense (Comptroller), in consultation with the Deputy Chief Management Officer of the Department of Defense, the Secretaries of the military departments, and the heads of the defense agencies and defense field activities, shall include a detailed description of the subordinate activities necessary to accomplish each interim milestone, including—

''(1) a justification of the time required for each activity;

''(2) metrics identifying the progress made within each activity; and

''(3) mitigating strategies for milestone timeframe slippages.

''(c) REPORT REQUIRED.—

''(1) IN GENERAL.—The Secretary of Defense shall submit to Congress a report relating to the Financial Improvement and Audit Readiness Plan of the Department of Defense submitted in accordance with section 1003 of the National Defense Authorization Act for 2010 (Public Law 111–84; 123 Stat. 2440 [2439]; 10 U.S.C. 2222 note) and section 881 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 121 Stat. 4306; 10 U.S.C. 2222 note).

''(2) MATTERS COVERED.—The report shall include a corrective action plan for any identified weaknesses or deficiencies in the execution of the Financial Improvement and Audit Readiness Plan. The corrective action plan shall—

''(A) identify near- and long-term measures for resolving any such weaknesses or deficiencies;

''(B) assign responsibilities within the Department of Defense to implement such measures;

''(C) specify implementation steps for such measures; and

''(D) provide timeframes for implementation of such measures.''

[Pub. L. 113–291, div. A, title IX, §901(n)(1), Dec. 19, 2014, 128 Stat. 3469, formerly set out as a References note under section 131 of this title, which provided that, effective after Feb. 1, 2017, any reference to the Deputy Chief Management Officer of the Department of Defense was to be deemed to refer to the Under Secretary of Defense for Business Management and Information, was repealed by Pub. L. 115–91, div. A, title X, §1081(b)(1)(D), Dec. 12, 2017, 131 Stat. 1597, effective as of Dec. 23, 2016.]

Pub. L. 111–383, div. A, title VIII, §881, Jan. 7, 2011, 124 Stat. 4306, as amended by Pub. L. 113–291, div. A, title IX, §901(n)(1), Dec. 19, 2014, 128 Stat. 3469; Pub. L. 115–91, div. A, title X, §1081(b)(1)(D), Dec. 12, 2017, 131 Stat. 1597, provided that:

''(a) INTERIM MILESTONES.—

''(1) REQUIREMENT.—Not later than 90 days after the date of the enactment of this Act [Jan. 7, 2011], the Under Secretary of Defense (Comptroller), in consultation with the Deputy Chief Management Officer of the Department of Defense, the secretaries of the military departments, and the heads of the defense agencies and defense field activities, shall establish interim milestones for achieving audit readiness of the financial statements of the Department of Defense, consistent with the requirements of section 1003 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note).

''(2) MATTERS INCLUDED.—The interim milestones established pursuant to paragraph (1) shall include, at a minimum, for each military department and for the defense agencies and defense field activities—

''(A) an interim milestone for achieving audit readiness for each major element of the statement of budgetary resources, including civilian pay, military pay, supply orders, contracts, and funds balance with the Treasury; and

''(B) an interim milestone for addressing the existence and completeness of each major category of Department of Defense assets, including military equipment, real property, inventory, and operating material and supplies.

''(3) DESCRIPTION IN SEMIANNUAL REPORTS.—The Under Secretary shall describe each interim milestone established pursuant to paragraph (1) in the next semiannual report submitted pursuant to section 1003(b) of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note). Each subsequent semiannual report submitted pursuant to section 1003(b) shall explain how the Department has progressed toward meeting such interim milestones.

''(b) VALUATION OF DEPARTMENT OF DEFENSE ASSETS.—

''(1) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act, the Under Secretary of Defense (Comptroller) shall, in consultation with other appropriate Federal agencies and officials—

''(A) examine the costs and benefits of alternative approaches to the valuation of Department of Defense assets;

''(B) select an approach to such valuation that is consistent with principles of sound financial management and the conservation of taxpayer resources; and

''(C) begin the preparation of a business case analysis supporting the selected approach.

''(2) The Under Secretary shall include information on the alternatives considered, the selected approach, and the business case analysis supporting that approach in the next semiannual report submitted pursuant to section 1003(b) of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note).

''(c) REMEDIAL ACTIONS REQUIRED.—In the event that the Department of Defense, or any component of the Department of Defense, is unable to meet an interim milestone established pursuant to subsection (a), the Under Secretary of Defense (Comptroller) shall—

''(1) develop a remediation plan to ensure that—

''(A) the component will meet the interim milestone no more than one year after the originally scheduled date; and

''(B) the component's failure to meet the interim milestone will not have an adverse impact on the Department's ability to carry out the plan under section 1003(a) of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note); and

''(2) include in the next semiannual report submitted pursuant to section 1003(b) of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note)—

''(A) a statement of the reasons why the Department of Defense, or component of the Department of Defense, will be unable to meet such interim milestone;

''(B) the revised completion date for meeting such interim milestone; and

''(C) a description of the actions that have been taken and are planned to be taken by the Department of Defense, or component of the Department of Defense, to meet such interim milestone.

''(d) INCENTIVES FOR ACHIEVING AUDITABILITY.—

''(1) REVIEW REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Under Secretary of Defense (Comptroller) shall review options for providing appropriate incentives to the military departments, Defense Agencies, and defense field

activities to ensure that financial statements are validated as ready for audit earlier than September 30, 2017.

''(2) OPTIONS REVIEWED.—The review performed pursuant to paragraph (1) shall consider changes in policy that reflect the increased confidence that can be placed in auditable financial statements, and shall include, at a minimum, consideration of the following options:

''(A) Consistent with the need to fund urgent warfighter requirements and operational needs, priority in the release of appropriated funds.

''(B) Relief from the frequency of financial reporting in cases in which such reporting is not required by law.

''(C) Relief from departmental obligation and expenditure thresholds to the extent that such thresholds establish requirements more restrictive than those required by law.

''(D) Increases in thresholds for reprogramming of funds.

''(E) Personnel management incentives for the financial and business management workforce.

''(F) Such other measures as the Under Secretary considers appropriate.

''(3) REPORT.—The Under Secretary shall include a discussion of the review performed pursuant to paragraph (1) in the next semiannual report pursuant to section 1003(b) of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2439; 10 U.S.C. 2222 note) and for each option considered pursuant to paragraph (2) shall include—

''(A) an assessment of the extent to which the implementation of the option—

''(i) would be consistent with the efficient operation of the Department of Defense and the effective funding of essential Department of Defense programs and activities; and

''(ii) would contribute to the achievement of Department of Defense goals to prepare auditable financial statements; and

''(B) a recommendation on whether such option should be adopted, a schedule for implementing the option if adoption is recommended, or a reason for not recommending the option if adoption is not recommended.''

[Pub. L. 113–291, div. A, title IX, §901(n)(1), Dec. 19, 2014, 128 Stat. 3469, formerly set out as a References note under section 131 of this title, which provided that, effective after Feb. 1, 2017, any reference to the Deputy Chief Management Officer of the Department of Defense was to be deemed to refer to the Under Secretary of Defense for Business Management and Information, was repealed by Pub. L. 115–91, div. A, title X, §1081(b)(1)(D), Dec. 12, 2017, 131 Stat. 1597, effective as of Dec. 23, 2016.]

Pub. L. 111–84, div. A, title X, §1003, Oct. 28, 2009, 123 Stat. 2439, as amended by Pub. L. 112–239, div. A, title X, §1005(a), Jan. 2, 2013, 126 Stat. 1904; Pub. L. 113–66, div. A, title X, §1003(b), Dec. 26, 2013, 127 Stat. 842, which directed the Chief Management Officer of the Department of Defense to develop a Financial Improvement and Audit Readiness Plan and to submit semi-annual reports to Congress on the status of the implementation of such plan, was repealed by Pub. L. 115–91, div. A, title X, §1002(c)(4), Dec. 12, 2017, 131 Stat. 1540.

BUSINESS PROCESS REENGINEERING EFFORTS; ONGOING PROGRAMS

Pub. L. 111–84, div. A, title X, §1072(b), Oct. 28, 2009, 123 Stat. 2471, provided that:

''(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act [Oct. 28, 2009], the appropriate chief management officer for each defense business system modernization approved by the Defense Business Systems Management Committee before the date of the enactment of this Act that will have a total cost in excess of $100,000,000 shall review such defense business system modernization to determine whether or not appropriate business process reengineering efforts have been undertaken to ensure that—

''(A) the business process to be supported by such defense business system modernization will be as streamlined and efficient as practicable; and

''(B) the need to tailor commercial-off-the-shelf systems to meet unique requirements or incorporate unique interfaces has been eliminated or reduced to the maximum extent practicable.

''(2) ACTION ON FINDING OF LACK OF REENGINEERING EFFORTS.—If the appropriate chief management officer determines that appropriate business process reengineering efforts have not been undertaken with regard to a defense business system modernization as described in paragraph (1), that chief management officer—

''(A) shall develop a plan to undertake business process reengineering efforts with respect to the defense business system modernization; and

''(B) may direct that the defense business system modernization be restructured or terminated, if necessary to meet the requirements of paragraph (1).

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

''(A) The term 'appropriate chief management officer', with respect to a defense business system modernization, has the meaning given that term in paragraph (2) of [former] subsection (f) of section 2222 of title 10, United States Code (as amended by subsection (a)(2) of this section).

''(B) The term 'defense business system modernization' has the meaning given that term in [former] subsection (j)(3) of section 2222 of title 10, United States Code.''

BUSINESS TRANSFORMATION INITIATIVES FOR THE MILITARY DEPARTMENTS

Pub. L. 110–417, [div. A], title IX, §908, Oct. 14, 2008, 122 Stat. 4569, provided that:

''(a) IN GENERAL.—The Secretary of each military department shall, acting through the Chief Management Officer of such military department, carry out an initiative for the business transformation of such military department.

''(b) OBJECTIVES.—The objectives of the business transformation initiative of a military department under this section shall include, at a minimum, the following:

''(1) The development of a comprehensive business transformation plan, with measurable performance goals and objectives, to achieve an integrated management system for the business operations of the military department.

''(2) The development of a well-defined enterprise-wide business systems architecture and transition plan encompassing end-to-end business processes and capable of providing accurately and timely information in support of business decisions of the military department.

''(3) The implementation of the business transformation plan developed pursuant to paragraph (1) and the business systems architecture and transition plan developed pursuant to paragraph (2).

''(c) BUSINESS TRANSFORMATION OFFICES.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act [Oct. 14, 2008], the Secretary of each military department shall establish within such military department an office (to be known as the 'Office of Business Transformation' of such military department) to assist the Chief Management Officer of such military department in carrying out the initiative required by this section for such military department.

''(2) HEAD.—The Office of Business Transformation of a military department under this subsection shall be headed by a Director of Business Transformation, who shall be appointed by the Chief Management Officer of the military department, in consultation with the Director of the Business Transformation Agency of the Department of Defense, from among individuals with significant experience managing large-scale organizations or business transformation efforts.

''(3) SUPERVISION.—The Director of Business Transformation of a military department under paragraph (2) shall report directly to the Chief Management Officer of the military department, subject to policy guidance from the Director of the Business Transformation Agency of the Department of Defense.

''(4) AUTHORITY.—In carrying out the initiative required by this section for a military department, the Director of Business Transformation of the military department under paragraph (2) shall have the authority to require elements of the military department to carry out actions that are within the purpose and scope of the initiative.

''(d) RESPONSIBILITIES OF BUSINESS TRANSFORMATION OFFICES.—The Office of Business Transformation of a military department established pursuant to subsection (b) may be responsible for the following:

''(1) Transforming the budget, finance, accounting, and human resource operations of the military department in a manner that is consistent with the business transformation plan developed pursuant to subsection (b)(1).

''(2) Eliminating or replacing financial management systems of the military department that are inconsistent with the business systems architecture and transition plan developed pursuant to subsection (b)(2).

''(3) Ensuring that the business transformation plan and the business systems architecture and transition plan are implemented in a manner that is aggressive, realistic, and accurately measured.

''(4) Such other responsibilities as the Secretary of that military department determines are appropriate.

''(e) REQUIRED ELEMENTS.—In carrying out the initiative required by this section for a military department, the Chief Management Officer and the Director of Business Transformation of the military department shall ensure that each element of the initiative is consistent with—

''(1) the requirements of the Business Enterprise Architecture and Transition Plan developed by the Secretary of Defense pursuant to section 2222 of title 10, United States Code;

''(2) the Standard Financial Information Structure of the Department of Defense;

''(3) the Federal Financial Management Improvement Act of 1996 [section 101(f) [title VIII] of title I of div. A of Pub. L. 104–208, 31 U.S.C. 3512 note] (and the amendments made by that Act); and

''(4) other applicable requirements of law and regulation.

''(f) REPORTS ON IMPLEMENTATION.—

''(1) INITIAL REPORTS.—Not later than nine months after the date of the enactment of this Act [Oct. 14, 2008], the Chief Management Officer of each military department shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the actions taken, and on the actions planned to be taken, by such military department to implement the requirements of this section.

''(2) UPDATES.—Not later than March 1 of each of 2010, 2011, and 2012, the Chief Management Officer of each military department shall submit to the congressional defense committees a current update of the report submitted by such Chief Management Officer under paragraph (1).''

FINANCIAL MANAGEMENT TRANSFORMATION INITIATIVE FOR THE DEFENSE AGENCIES

Pub. L. 110–181, div. A, title X, § 1005, Jan. 28, 2008, 122 Stat. 301, provided that:

''(a) FINANCIAL MANAGEMENT TRANSFORMATION INITIATIVE.—

''(1) IN GENERAL.—The Director of the Business Transformation Agency of the Department of Defense shall carry out an initiative for financial management transformation in the Defense Agencies. The initiative shall be known as the 'Defense Agencies Initiative' (in this section referred to as the 'Initiative').

''(2) SCOPE OF AUTHORITY.—In carrying out the Initiative, the Director of the Business Transformation Agency may require the heads of the Defense Agencies to carry out actions that are within the purpose and scope of the Initiative.

''(b) PURPOSES.—The purposes of Initiative shall be as follows:

''(1) To eliminate or replace financial management systems of the Defense Agencies that are duplicative, redundant, or fail to comply with the standards set forth in subsection (d).

''(2) To transform the budget, finance, and accounting operations of the Defense Agencies to enable the Defense Agencies to achieve accurate and reliable financial information needed to support financial accountability and effective and efficient management decisions.

''(c) REQUIRED ELEMENTS.—The Initiative shall include, to the maximum extent practicable—

''(1) the utilization of commercial, off-the-shelf technologies and web-based solutions;

''(2) a standardized technical environment and an open and accessible architecture; and

''(3) the implementation of common business processes, shared services, and common data structures.

''(d) STANDARDS.—In carrying out the Initiative, the Director of the Business Transformation Agency shall ensure that the Initiative is consistent with—

''(1) the requirements of the Business Enterprise Architecture and Transition Plan developed pursuant to section 2222 of title 10, United States Code;

''(2) the Standard Financial Information Structure of the Department of Defense;

''(3) the Federal Financial Management Improvement Act of 1996 [section 101(f) [title VIII] of title I of div. A of Pub. L. 104–208, 31 U.S.C. 3512 note] (and the amendments made by that Act); and

''(4) other applicable requirements of law and regulation.

''(e) SCOPE.—The Initiative shall be designed to provide, at a minimum, capabilities in the major process areas for both general fund and working capital fund operations of the Defense Agencies as follows:

''(1) Budget formulation.

''(2) Budget to report, including general ledger and trial balance.

''(3) Procure to pay, including commitments, obligations, and accounts payable.

''(4) Order to fulfill, including billing and accounts receivable.

''(5) Cost accounting.

''(6) Acquire to retire (account management).

''(7) Time and attendance and employee entitlement.

''(8) Grants financial management.

''(f) CONSULTATION.—In carrying out subsections (d) and (e), the Director of the Business Transformation Agency shall consult with the Comptroller of the Department of Defense [now Under Secretary of Defense (Comptroller)] to ensure that any financial management systems developed for the Defense Agencies, and any changes to the budget, finance, and accounting operations of the Defense Agencies, are consistent with the financial standards and requirements of the Department of Defense.

''(g) PROGRAM CONTROL.—In carrying out the Initiative, the Director of the Business Transformation Agency shall establish—

''(1) a board (to be known as the 'Configuration Control Board') to manage scope and cost changes to the Initiative; and

''(2) a program management office (to be known as the 'Program Management Office') to control and enforce assumptions made in the acquisition plan, the cost estimate, and the system integration contract for the Initiative, as directed by the Configuration Control Board.

''(h) PLAN ON DEVELOPMENT AND IMPLEMENTATION OF INITIATIVE.—Not later than six months after the date of the enactment of this Act [Jan. 28, 2008], the Director of the Business Transformation Agency shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for the development and implementation of the Initiative. The plan shall provide for the implementation of an initial capability under the Initiative as follows:

''(1) In at least one Defense Agency by not later than eight months after the date of the enactment of this Act.

''(2) In not less than five Defense Agencies by not later than 18 months after the date of the enactment of this Act.''

LIMITATION ON FINANCIAL MANAGEMENT IMPROVEMENT AND AUDIT INITIATIVES WITHIN THE DEPARTMENT OF DEFENSE

Pub. L. 109–364, div. A, title III, § 321, Oct. 17, 2006, 120 Stat. 2144, as amended by Pub. L. 111–383, div. A, title X, § 1075(g)(1), Jan. 7, 2011, 124 Stat. 4376, provided that:

''(a) LIMITATION.—The Secretary of Defense may not obligate or expend any funds for the purpose of any financial management improvement activity relating to the preparation, processing, or auditing of financial statements until the Secretary submits to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written determination that each activity proposed to be funded is—

''(1) consistent with the financial management improvement plan of the Department of Defense required by section 376(a)(1) of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109–163; 119 Stat. 3213); and

''(2) likely to improve internal controls or otherwise result in sustained improvements in the ability of the Department to produce timely, reliable, and complete financial management information.

''(b) EXCEPTION.—The limitation in subsection (a) shall not apply to an activity directed exclusively at assessing the adequacy of internal controls and remediating any inadequacy identified pursuant to such assessment.''

TIME-CERTAIN DEVELOPMENT FOR DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY BUSINESS SYSTEMS

Pub. L. 109–364, div. A, title VIII, § 811, Oct. 17, 2006, 120 Stat. 2316, which provided limitations for Milestone A approval and initial operational capability regarding certain Department of Defense information technology business systems, was repealed by Pub. L. 114–92, div. A, title VIII, § 883(c), Nov. 25, 2015, 129 Stat. 947.

§ 2223. Information technology: additional responsibilities of Chief Information Officers

(a) ADDITIONAL RESPONSIBILITIES OF CHIEF INFORMATION OFFICER OF DEPARTMENT OF DEFENSE.—In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of the Department of Defense shall—

(1) review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems;

(2) ensure the interoperability of information technology and national security systems throughout the Department of Defense;

(3) ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed;

(4) provide for the elimination of duplicate information technology and national security systems within and between the military departments and Defense Agencies; and

(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

(b) ADDITIONAL RESPONSIBILITIES OF CHIEF INFORMATION OFFICER OF MILITARY DEPARTMENTS.—In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of a military department, with respect to the military department concerned, shall—

(1) review budget requests for all information technology and national security systems;

(2) ensure that information technology and national security systems are in compliance with standards of the Government and the Department of Defense;

(3) ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense; and

(4) coordinate with the Joint Staff with respect to information technology and national security systems.

(c) DEFINITIONS.—In this section:

(1) The term ''Chief Information Officer'' means the senior official designated by the Secretary of Defense or a Secretary of a military department pursuant to section 3506 of title 44.

(2) The term ''information technology'' has the meaning given that term by section 11101 of title 40.

(3) The term ''national security system'' has the meaning given that term by section 3552(b)(6) of title 44.

(Added Pub. L. 105–261, div. A, title III, § 331(a)(1), Oct. 17, 1998, 112 Stat. 1967; amended Pub. L. 106–398, § 1 [[div. A], title VIII, § 811(a)], Oct. 30, 2000, 114 Stat. 1654, 1654A–210; Pub. L. 107–217, § 3(b)(1), Aug. 21, 2002, 116 Stat. 1295; Pub. L. 109–364, div. A, title IX, § 906(b), Oct. 17, 2006, 120 Stat. 2354; Pub. L. 113–283, § 2(e)(5)(B), Dec. 18, 2014, 128 Stat. 3087; Pub. L. 114–92, div. A, title X, § 1081(a)(7), Nov. 25, 2015, 129 Stat. 1001.)

Editorial Notes

AMENDMENTS

2015—Subsec. (c)(3). Pub. L. 114–92 substituted ''section 3552(b)(6)'' for ''section 3552(b)(5)''.

2014—Subsec. (c)(3). Pub. L. 113–283 substituted ''section 3552(b)(5)'' for ''section 3542(b)(2)''.

2006—Subsec. (c)(3). Pub. L. 109–364 substituted ''section 3542(b)(2) of title 44'' for ''section 11103 of title 40''.

2002—Subsecs. (a), (b). Pub. L. 107–217, § 3(b)(1)(A), (B), substituted ''section 11315 of title 40'' for ''section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425)'' in introductory provisions.

Subsec. (c)(2). Pub. L. 107–217, § 3(b)(1)(C), substituted ''section 11101 of title 40'' for ''section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401)''.

Subsec. (c)(3). Pub. L. 107–217, § 3(b)(1)(D), substituted ''section 11103 of title 40'' for ''section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452)''.

2000—Subsec. (a)(5). Pub. L. 106–398 added par. (5).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Pub. L. 105–261, div. A, title III, § 331(b), Oct. 17, 1998, 112 Stat. 1968, provided that: ''Section 2223 of title 10, United States Code, as added by subsection (a), shall take effect on October 1, 1998.''

MODERNIZATION OF THE DEPARTMENT OF DEFENSE'S AUTHORIZATION TO OPERATE PROCESSES

Pub. L. 118–159, div. A, title XV, § 1522, Dec. 23, 2024, 138 Stat. 2140, provided that:

''(a) ACTIVE DIRECTORY OF AUTHORIZING OFFICIALS.—

''(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense and in coordination with the Chief Information Officers of the military departments, shall establish and regularly update a digital directory of all authorizing officials in the military departments.

''(2) CONTENTS.—The directory established under paragraph (1) shall include—

''(A) the most current contact information for such authorizing official; and

''(B) a list of each training required to perform the duties and responsibilities of an authorizing official completed by such authorizing official.

''(b) PRESUMPTION OF RECIPROCAL SOFTWARE ACCREDITING STANDARDS.—

''(1) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall implement a policy that requires authorizing officials to adopt the security analysis and artifacts, as appropriate, of a cloud-hosted platform, service, or application that has already been authorized by another authorizing official in the Department of Defense in order to more rapidly adopt and use such cloud-hosted platforms, services, and applications, at the corresponding classification level and in accordance with the existing authorization conditions, without additional authorizations or reviews.

''(2) ELEMENTS.—The Secretary shall ensure that the policy implemented under paragraph (1)—

''(A) ensures the development of standardized and transparent documentation of the security, accreditation, performance, and operational capabilities of cloud-hosted platforms, services, and applications to enable decision making by mission owners of such cloud-hosted platforms, services, and applications;

''(B) provides for an intuitive and digital workflow to document acknowledgments among mission owners and system owners of use of the operational capabilities of cloud-hosted platforms, services, and applications;

''(C) directs a review by mission owners of existing authorization information, at the appropriate classification level, regarding the status of the operational capabilities of cloud-hosted platforms, services, and applications, including through management dashboards or other management analytic capabilities; and

''(D) defines a process, including required timelines, to allow authorizing officials that disagree with the security analysis of a cloud-hosted platform, service, or application that such official would be required to adopt under such policy to present such disagreement to the Chief Information Officer of the Department of Defense, or such other individual or entity designated by the Chief Information Officer, for adjudication.

''(3) APPLICABILITY.—The policy implemented pursuant to subsection (a) shall apply to—

''(A) all authorizing officials in the Department of Defense, including in each military department, component, and agency of the Department; and

''(B) all operational capabilities of cloud-hosted platforms, services, and applications, including capabilities on public cloud infrastructure, as authorized through the Federal Risk and Authorization Management Program established under section 3608 of title 44, United States Code, and the Defense Information Systems Agency, and capabilities on private cloud landing zones managed by the Department of Defense that are authorized by Department accrediting officials.

''(c) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the status of the implementation of subsections (a) and (b).

''(d) DEFINITIONS.—In this section—

''(1) the term 'Authorization to Operate' has the meaning given such term in the Office of Management and Budget Circular A-130;

''(2) the term 'authorizing official' means an officer who is authorized to assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the United States;

''(3) the term 'military departments' has the meaning given such term in section 101(a) of title 10, United States Code;

''(4) the term 'mission owner' means the user of a cloud-based platform, service, or application; and

''(5) the term 'system owner' means the element of the Department of Defense responsible for acquiring a cloud-based platform, service, or application, but which is not a mission owner of such cloud-based platform, service, or application.''

REQUIRED POLICIES TO ESTABLISH DATALINK STRATEGY OF DEPARTMENT OF DEFENSE

Pub. L. 118–31, div. A, title XV, § 1527, Dec. 22, 2023, 137 Stat. 559, provided that:

''(a) POLICIES REQUIRED.—

''(1) IN GENERAL.—The Secretary of Defense shall develop and implement policies to establish a unified datalink strategy of the Department of Defense (in this section referred to as the 'strategy').

''(2) ELEMENTS.—The policies under paragraph (1) shall provide for, at a minimum, the following:

''(A) The designation of an organization to serve as the lead coordinator of datalink activities throughout the Department of Defense.

''(B) The prioritization and coordination across the military departments with respect to the strategy within the requirements generation process of the Department.

''(C) The use throughout the Department of a common standardized datalink network or transport protocol that ensures interoperability between independently developed datalinks, regardless of physical medium used, and ensures mesh routing. In developing such policy, the Secretary of Defense shall consider the use of a subset of Internet Protocol.

''(D) A programmatic decoupling of the physical method used to transmit data, the network or transport protocols used in the transmission and reception of data, and the applications used to process and use data.

''(E) Coordination of the strategy with respect to weapon systems executing the same mission types across the military departments, including through the use of a common set of datalink waveforms. In developing such policy, the Secretary shall evaluate the use of redundant datalinks for line-of-sight and beyond-line-of-sight information exchange for each weapon systems platform.

''(F) Coordination between the Department and the intelligence community (as such term is defined in section 3 of the National Security Act of

1947 (50 U.S.C. 3003)) to leverage any efficiencies and overlap with existing datalink waveforms of the intelligence community.

''(G) Methods to support the rapid integration of common datalinks across the military departments.

''(H) Support for modularity of specific datalink waveforms to enable rapid integration of future datalinks, including the use of software defined radios compliant with modular open system architecture and sensor open system architecture.

''(b) INFORMATION TO CONGRESS.—Not later than June 1, 2024, the Secretary of Defense shall—

''(1) provide to the appropriate congressional committees a briefing on the proposed policies under subsection (a)(1), including timelines for the implementation of such policies; and

''(2) submit to the appropriate congressional committees—

''(A) an estimated timeline for the implementations of datalinks;

''(B) a list of any additional resources and authorities necessary to implement the strategy; and

''(C) a determination of whether a common set of datalinks can and should be implemented across all major weapon systems (as such term is defined in section 3455 of title 10, United States Code) of the Department of Defense.

''(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] and the congressional intelligence committees, as such term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).''

DEMONSTRATION PROGRAM FOR COMPONENT CONTENT MANAGEMENT SYSTEMS

Pub. L. 117–263, div. A, title IX, §917, Dec. 23, 2022, 136 Stat. 2756, provided that:

''(a) IN GENERAL.—Not later than July 1, 2023, the Chief Information Officer of the Department of Defense, in coordination with the official designated under section 238(b) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. note prec. 4061), shall complete a pilot program to demonstrate the application of component content management systems to a distinct set of data of the Department.

''(b) SELECTION OF DATA SET.—In selecting a distinct set of data of the Department for purposes of the pilot program required by subsection (a), the Chief Information Officer shall consult with, at a minimum, the following:

''(1) The Office of the Secretary of Defense, with respect to directives, instructions, and other regulatory documents of the Department.

''(2) The Office of the Secretary of Defense and the Joint Staff, with respect to execution orders.

''(3) The Office of the Under Secretary of Defense for Research and Engineering and the military departments, with respect to technical manuals.

''(4) The Office of the Under Secretary of Defense for Acquisition and Sustainment, with respect to Contract Data Requirements List documents.

''(c) AUTHORITY TO ENTER INTO CONTRACTS.—Subject to the availability of appropriations, the Secretary of Defense may enter into contracts or other agreements with public or private entities to conduct studies and demonstration projects under the pilot program required by subsection (a).

''(c) [sic] BRIEFING REQUIRED.—Not later than 60 days after the date of the enactment of this Act [Dec. 23, 2022], the Chief Information Officer shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on plans to implement the pilot program required by subsection (a).

''(d) COMPONENT CONTENT MANAGEMENT SYSTEM DEFINED.—In this section, the term 'component content management system' means any content management system that enables the management of content at a component level instead of at the document level.''

IMPROVED MANAGEMENT OF INFORMATION TECHNOLOGY AND CYBERSPACE INVESTMENTS

Pub. L. 116–92, div. A, title VIII, §892, Dec. 20, 2019, 133 Stat. 1539, provided that:

''(a) IMPROVED MANAGEMENT.—

''(1) IN GENERAL.—The Chief Information Officer of the Department of Defense shall work with the Chief Data Officer of the Department of Defense to optimize the Department's process for accounting for, managing, and reporting its information technology and cyberspace investments. The optimization should include alternative methods of presenting budget justification materials to the public and congressional staff to more accurately communicate when, how, and with what frequency capability is delivered to end users, in accordance with best practices for managing and reporting on information technology investments.

''(2) BRIEFING.—Not later than February 3, 2020, the Chief Information Officer of the Department of Defense shall brief the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] on the process optimization undertaken pursuant to paragraph (1), including any recommendations for legislation.

''(b) DELIVERY OF INFORMATION TECHNOLOGY BUDGET.—The Secretary of Defense shall submit to the congressional defense committees the Department of Defense budget request for information technology not later than 15 days after the submittal to Congress of the budget of the President for a fiscal year pursuant to section 1105 of title 31, United States Code.''

CHIEF DATA OFFICER RESPONSIBILITY FOR DOD DATA SETS

Pub. L. 116–92, div. A, title IX, §903(b), Dec. 20, 2019, 133 Stat. 1555, as amended by Pub. L. 117–263, div. A, title II, §212(k), Dec. 23, 2022, 136 Stat. 2470, provided that:

''(1) IN GENERAL.—In addition to any other functions and responsibilities specified in section 3520(c) of title 44, United States, Code, the Chief Data Officer of the Department of Defense shall also be the official in the Department of Defense with principal responsibility for providing for the availability of common, usable, Defense-wide data sets.

''(2) ACCESS TO ALL DOD DATA.—In order to carry out the responsibility specified in paragraph (1), the Chief Data Officer shall have access to all Department of Defense data, including data in connection with warfighting missions and back-office data.

''(3) REPORT.—Not later than December 1, 2019, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report setting forth such recommendations for legislative or administrative action as the Secretary considers appropriate to carry out this subsection.''

PILOT PROGRAM FOR OPEN SOURCE SOFTWARE

Pub. L. 115–91, div. A, title VIII, §875, Dec. 12, 2017, 131 Stat. 1503, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall initiate for the Department of Defense the open source software pilot program established by the Office of Management and Budget Memorandum M-16-21 titled 'Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software' and dated August 8, 2016.

''(b) REPORT TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense shall provide a report to Congress

with details of the plan of the Department of Defense to implement the pilot program required by subsection (a). Such plan shall include identifying candidate software programs, selection criteria, intellectual property and licensing issues, and other matters determined by the Secretary.

''(c) COMPTROLLER GENERAL REPORT.—Not later than June 1, 2019, the Comptroller General of the United States shall provide a report to Congress on the implementation of the pilot program required by subsection (a) by the Secretary of Defense. The report shall address, at a minimum, the compliance of the Secretary with the requirements of the Office of Management and Budget Memorandum M-16-21, the views of various software and information technology stakeholders in the Department of Defense, and any other matters determined by the Comptroller General.''

PILOT PROGRAM ON EVALUATION OF COMMERCIAL INFORMATION TECHNOLOGY

Pub. L. 114–328, div. A, title II, §232, Dec. 23, 2016, 130 Stat. 2061, provided that:

''(a) PILOT PROGRAM.—The Director of the Defense Information Systems Agency may carry out a pilot program to evaluate commercially available information technology tools to better understand the potential impact of such tools on networks and computing environments of the Department of Defense.

''(b) ACTIVITIES.—Activities under the pilot program may include the following:

''(1) Prototyping, experimentation, operational demonstration, military user assessments, and other means of obtaining quantitative and qualitative feedback on the commercial information technology products.

''(2) Engagement with the commercial information technology industry to—

''(A) forecast military requirements and technology needs; and

''(B) support the development of market strategies and program requirements before finalizing acquisition decisions and strategies.

''(3) Assessment of novel or innovative commercial technology for use by the Department of Defense.

''(4) Assessment of novel or innovative contracting mechanisms to speed delivery of capabilities to the Armed Forces.

''(5) Solicitation of operational user input to shape future information technology requirements of the Department of Defense.

''(c) LIMITATION ON AVAILABILITY OF FUNDS.—Of the amounts authorized to be appropriated for research, development, test, and evaluation, Defense-wide, for each of fiscal years 2017 through 2022, not more than $15,000,000 may be expended on the pilot program in any such fiscal year.''

ADDITIONAL REQUIREMENTS RELATING TO THE SOFTWARE LICENSES OF THE DEPARTMENT OF DEFENSE

Pub. L. 113–66, div. A, title IX, §935, Dec. 26, 2013, 127 Stat. 833, provided that:

''(a) UPDATED PLAN.—

''(1) UPDATE.—The Chief Information Officer of the Department of the Defense shall, in consultation with the chief information officers of the military departments and the Defense Agencies, update the plan for the inventory of selected software licenses of the Department of Defense required under section 937 of the National Defense Authorization Act for 2013 [probably means the National Defense Authorization Act for Fiscal Year 2013] (Public Law 112–239; 10 U.S.C. 2223 note) to include a plan for the inventory of all software licenses of the Department of Defense for which a military department spends more than $5,000,000 annually on any individual title, including a comparison of licenses purchased with licenses in use.

''(2) ELEMENTS.—The update required under paragraph (1) shall—

''(A) include plans for implementing an automated solution capable of reporting the software license compliance position of the Department and providing a verified audit trail, or an audit trail otherwise produced and verified by an independent third party;

''(B) include details on the process and business systems necessary to regularly perform reviews, a procedure for validating and reporting deregistering and registering new software, and a mechanism and plan to relay that information to the appropriate chief information officer; and

''(C) a proposed timeline for implementation of the updated plan in accordance with paragraph (3).

''(3) SUBMISSION.—Not later than September 30, 2015, the Chief Information Officer of the Department of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the updated plan required under paragraph (1).

''(b) PERFORMANCE PLAN.—If the Chief Information Officer of the Department of Defense determines through the implementation of the process and business systems in the updated plan required by subsection (a) that the number of software licenses of the Department for an individual title for which a military department spends greater than $5,000,000 annually exceeds the needs of the Department for such software licenses, or the inventory discloses that there is a discrepancy between the number of software licenses purchased and those in actual use, the Chief Information Officer of the Department of Defense shall implement a plan to bring the number of such software licenses into balance with the needs of the Department and the terms of any relevant contract.''

COLLECTION AND ANALYSIS OF NETWORK FLOW DATA

Pub. L. 112–239, div. A, title IX, §935, Jan. 2, 2013, 126 Stat. 1886, provided that:

''(a) DEVELOPMENT OF TECHNOLOGIES.—The Chief Information Officer of the Department of Defense may, in coordination with the Under Secretary of Defense for Policy and the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security] and acting through the Director of the Defense Information Systems Agency, use the available funding and research activities and capabilities of the Community Data Center of the Defense Information Systems Agency to develop and demonstrate collection, processing, and storage technologies for network flow data that—

''(1) are potentially scalable to the volume used by Tier 1 Internet Service Providers to collect and analyze the flow data across their networks;

''(2) will substantially reduce the cost and complexity of capturing and analyzing high volumes of flow data; and

''(3) support the capability—

''(A) to detect and identify cyber security threats, networks of compromised computers, and command and control sites used for managing illicit cyber operations and receiving information from compromised computers;

''(B) to track illicit cyber operations for attribution of the source; and

''(C) to provide early warning and attack assessment of offensive cyber operations.

''(b) COORDINATION.—Any research and development required in the development of the technologies described in subsection (a) shall be conducted in cooperation with the heads of other appropriate departments and agencies of the Federal Government and, whenever feasible, Tier 1 Internet Service Providers and other managed security service providers.''

COMPETITION FOR LARGE-SCALE SOFTWARE DATABASE AND DATA ANALYSIS TOOLS

Pub. L. 112–239, div. A, title IX, §936, Jan. 2, 2013, 126 Stat. 1886, provided that:

''(a) ANALYSIS.—

''(1) REQUIREMENT.—The Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall conduct an analysis of large-scale software database tools and large-scale software data analysis tools that could be used to meet current and future Department of Defense needs for large-scale data analytics.

''(2) ELEMENTS.—The analysis required under paragraph (1) shall include—

''(A) an analysis of the technical requirements and needs for large-scale software database and data analysis tools, including prioritization of key technical features needed by the Department of Defense; and

''(B) an assessment of the available sources from Government and commercial sources to meet such needs, including an assessment by the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy to ensure sufficiency and diversity of potential commercial sources.

''(3) SUBMISSION.—Not later than 180 days after the date of the enactment of this Act [Jan. 2, 2013], the Chief Information Officer shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the results of the analysis required under paragraph (1).

''(b) COMPETITION REQUIRED.—

''(1) IN GENERAL.—If, following the analysis required under subsection (a), the Chief Information Officer of the Department of Defense identifies needs for software systems or large-scale software database or data analysis tools, the Department shall acquire such systems or such tools based on market research and using competitive procedures in accordance with applicable law and the Defense Federal Acquisition Regulation Supplement.

''(2) NOTIFICATION.—If the Chief Information Officer elects to acquire large-scale software database or data analysis tools using procedures other than competitive procedures, the Chief Information Officer and the Under Secretary of Defense for Acquisition, Technology, and Logistics shall submit a written notification to the congressional defense committees on a quarterly basis until September 30, 2018, that describes the acquisition involved, the date the decision was made, and the rationale for not using competitive procedures.''

SOFTWARE LICENSES OF THE DEPARTMENT OF DEFENSE

Pub. L. 112–239, div. A, title IX, § 937, Jan. 2, 2013, 126 Stat. 1887, provided that:

''(a) PLAN FOR INVENTORY OF LICENSES.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Jan. 2, 2013], the Chief Information Officer of the Department of the [sic] Defense shall, in consultation with the chief information officers of the military departments and the Defense Agencies, issue a plan for the inventory of selected software licenses of the Department of Defense, including a comparison of licenses purchased with licenses installed.

''(2) SELECTED SOFTWARE LICENSES.—The Chief Information Officer shall determine the software licenses to be treated as selected software licenses of the Department for purposes of this section. The licenses shall be determined so as to maximize the return on investment in the inventory conducted pursuant to the plan required by paragraph (1).

''(3) PLAN ELEMENTS.—The plan under paragraph (1) shall include the following:

''(A) An identification and explanation of the software licenses determined by the Chief Information Officer under paragraph (2) to be selected software licenses for purposes of this section, and a summary outline of the software licenses determined not to be selected software licenses for such purposes.

''(B) Means to assess the needs of the Department and the components of the Department for selected software licenses during the two fiscal years following the date of the issuance of the plan.

''(C) Means by which the Department can achieve the greatest possible economies of scale and cost savings in the procurement, use, and optimization of selected software licenses.

''(b) PERFORMANCE PLAN.—If the Chief Information Officer determines through the inventory conducted pursuant to the plan required by subsection (a) that the number of selected software licenses of the Department and the components of the Department exceeds the needs of the Department for such software licenses, the Secretary of Defense shall implement a plan to bring the number of such software licenses into balance with the needs of the Department.''

OZONE WIDGET FRAMEWORK

Pub. L. 112–81, div. A, title IX, § 924, Dec. 31, 2011, 125 Stat. 1539, provided that:

''(a) MECHANISM FOR INTERNET PUBLICATION OF INFORMATION FOR DEVELOPMENT OF ANALYSIS TOOLS AND APPLICATIONS.—The Chief Information Officer of the Department of Defense, acting through the Director of the Defense Information Systems Agency, shall implement a mechanism to publish and maintain on the public Internet the application programming interface specifications, a developer's toolkit, source code, and such other information on, and resources for, the Ozone Widget Framework (OWF) as the Chief Information Officer considers necessary to permit individuals and companies to develop, integrate, and test analysis tools and applications for use by the Department of Defense and the elements of the intelligence community.

''(b) PROCESS FOR VOLUNTARY CONTRIBUTION OF IMPROVEMENTS BY PRIVATE SECTOR.—In addition to the requirement under subsection (a), the Chief Information Officer shall also establish a process by which private individuals and companies may voluntarily contribute the following:

''(1) Improvements to the source code and documentation for the Ozone Widget Framework.

''(2) Alternative or compatible implementations of the published application programming interface specifications for the Framework.

''(c) ENCOURAGEMENT OF USE AND DEVELOPMENT.—The Chief Information Officer shall, whenever practicable, encourage and foster the use, support, development, and enhancement of the Ozone Widget Framework by the computer industry and commercial information technology vendors, including the development of tools that are compatible with the Framework.''

CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY

Pub. L. 111–383, div. A, title IX, § 931, Jan. 7, 2011, 124 Stat. 4334, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to work, in coordination with the Chief Information Officers of the military departments and the Defense Agencies and with senior cybersecurity and information assurance officials within the Department of Defense and otherwise within the Federal Government, to achieve, to the extent practicable, the following:

''(1) The continuous prioritization of the policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

''(2) The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the

compliance of that infrastructure with such policies, procedures, and practices, including automation of—

''(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(c) of title 44, United States Code; and

''(B) management, operational, and technical controls relied on for evaluations under [former] section 3545 of title 44, United States Code [see now 44 U.S.C. 3555].

''(b) DEFINITIONS.—In this section:

''(1) The term 'information security incident' means an occurrence that—

''(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

''(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

''(2) The term 'information infrastructure' means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

''(3) The term 'national security system' has the meaning given that term in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].''

[§ 2223a. Renumbered § 4571]

§ 2224. Defense Information Assurance Program

(a) DEFENSE INFORMATION ASSURANCE PROGRAM.—The Secretary of Defense shall carry out a program, to be known as the ''Defense Information Assurance Program'', to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis.

(b) OBJECTIVES OF THE PROGRAM.—The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

(c) PROGRAM STRATEGY.—In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure, including through compliance with subchapter II of chapter 35 of title 44, including through compliance with subchapter III of chapter 35 of title 44. The program strategy shall include the following:

(1) A vulnerability and threat assessment of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the armed forces.

(2) Development of essential information assurances technologies and programs.

(3) Organization of the Department, the armed forces, and supporting activities to defend against information warfare.

(4) Joint activities of the Department with other departments and agencies of the Government, State and local agencies, and elements of the national information infrastructure.

(5) The conduct of exercises, war games, simulations, experiments, and other activities designed to prepare the Department to respond to information warfare threats.

(6) Development of proposed legislation that the Secretary considers necessary for implementing the program or for otherwise responding to the information warfare threat.

(d) COORDINATION.—In carrying out the program, the Secretary shall coordinate, as appropriate, with the head of any relevant Federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department and the armed forces on information assurance measures necessary to the protection of these systems.

[(e) Repealed. Pub. L. 108–136, div. A, title X, § 1031(a)(12), Nov. 24, 2003, 117 Stat. 1597.]

(f) INFORMATION ASSURANCE TEST BED.—The Secretary shall develop an information assurance test bed within the Department of Defense to provide—

(1) an integrated organization structure to plan and facilitate the conduct of simulations, war games, exercises, experiments, and other activities to prepare and inform the Department regarding information warfare threats; and

(2) organization and planning means for the conduct by the Department of the integrated or joint exercises and experiments with elements of the national information systems infrastructure and other non-Department of Defense organizations that are responsible for the oversight and management of critical information systems and infrastructures on which the Department, the armed forces, and supporting activities depend for the conduct of daily operations and operations during crisis.

(Added Pub. L. 106–65, div. A, title X, § 1043(a), Oct. 5, 1999, 113 Stat. 760; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1063], Oct. 30, 2000, 114 Stat. 1654, 1654A–274; Pub. L. 107–296, title X, § 1001(c)(1)(B), Nov. 25, 2002, 116 Stat. 2267; Pub. L. 107–347, title III, § 301(c)(1)(B), Dec. 17, 2002, 116 Stat. 2955; Pub. L. 108–136, div. A, title X, § 1031(a)(12), Nov. 24, 2003, 117 Stat. 1597; Pub. L. 108–375, div. A, title X, § 1084(d)(17), Oct. 28, 2004, 118 Stat. 2062.)

Editorial Notes

AMENDMENTS

2004—Subsec. (c). Pub. L. 108–375 substituted ''subchapter II'' for ''subtitle II'' in introductory provisions.

2003—Subsec. (e). Pub. L. 108–136 struck out subsec. (e) which directed the Secretary of Defense to annually submit to Congress a report on the Defense Information Assurance Program.

2002—Subsec. (b). Pub. L. 107–296, § 1001(c)(1)(B)(i), and Pub. L. 107–347, § 301(c)(1)(B)(i), amended subsec. (b) identically, substituting ''Objectives of the Program'' for ''Objectives and Minimum Requirements'' in heading and striking out par. (1) designation before ''The objectives''.

Subsec. (b)(2). Pub. L. 107–347, § 301(c)(1)(B)(ii), struck out par. (2) which read as follows: ''The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44.''

Pub. L. 107–296, § 1001(c)(1)(B)(ii), which directed the striking out of ''(2) the program shall at a minimum

meet the requirements of section 3534 and 3535 of title 44, United States Code.'' could not be executed. See above par.

Subsec. (c). Pub. L. 107–347, §301(c)(1)(B)(iii), inserted '', including through compliance with subchapter III of chapter 35 of title 44'' after ''infrastructure'' in introductory provisions.

Pub. L. 107–296, §1001(c)(1)(B)(iii), inserted '', including through compliance with subtitle II of chapter 35 of title 44'' after ''infrastructure'' in introductory provisions.

2000—Subsec. (b). Pub. L. 106–398, §1 [[div. A], title X, §1063(a)], substituted ''OBJECTIVES AND MINIMUM REQUIREMENTS'' for ''OBJECTIVES OF THE PROGRAM'' in heading, designated existing provisions as par. (1), and added par. (2).

Subsec. (e)(7). Pub. L. 106–398, §1 [[div. A], title X, §1063(b)], added par. (7).

Statutory Notes and Related Subsidiaries

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.

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of Title 44, Public Printing and Documents.

USABILITY OF ANTIQUATED AND PROPRIETARY DATA FORMATS FOR MODERN OPERATIONS

Pub. L. 118–159, div. A, title XV, §1521, Dec. 23, 2024, 138 Stat. 2138, provided that:

''(a) STRATEGY AND ROADMAP.—

''(1) IN GENERAL.—Not later than 270 days after the date of enactment of this Act [Dec. 23, 2024], the Secretary of Defense, in coordination with the Secretaries of the military departments, shall develop—

''(A) a strategy for the Department of Defense, including each of the military departments, to identify, implement, and use modern data formats as the primary method of electronic communication for command and control activities and for weapon systems, including sensors associated with such weapon systems; and

''(B) an associated five-year roadmap for the Department of Defense, including each of the military departments, to implement modern data formats under the strategy described in subparagraph (A).

''(2) ELEMENTS.—The strategy and roadmap required under paragraph (1) shall include the following elements:

''(A) The activities of the Chief Digital and Artificial Intelligence Officer of the Department of Defense to increase and synchronize the use of modern data formats and modern data sharing standards across the Department of Defense.

''(B) Development of standard definitions for modern and antiquated data formats, including a representative catalog of the types of data formats that fall under each category.

''(C) The activities of the military departments to increase the use of modern data formats and modern data sharing standards for command and control systems, weapon systems, and sensors associated with such weapon systems.

''(D) An identification of barriers to the use of modern data formats and modern data sharing standards within weapon systems and sensors associated with such weapon systems across the Department of Defense.

''(E) An identification of barriers to the use of modern data formats and modern data sharing standards within command and control systems across the Department of Defense.

''(F) An identification of limitations on combined joint all-domain command and control capabilities resulting from the use of antiquated data formats.

''(G) An identification of policy documents, instructions, or other guidance requiring an update pursuant to such strategy.

''(H) The sources of funding for each military department with respect to implementation of such strategy.

''(3) SUBMISSION TO CONGRESS.—Upon completion of the strategy and roadmap required under this subsection, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives such strategy.

''(4) MODERN DATA FORMATS.—For the purposes of this subsection, the term 'modern data formats' includes—

''(A) the JavaScript Object Notation data format;

''(B) the Binary JavaScript Object Notation data format;

''(C) the Protocol Buffers data format; and

''(D) such other data formats that the Secretary of Defense determines would meet the requirements in this section.

''(b) PILOT PROGRAMS.—

''(1) ESTABLISHMENT.—Not later than 60 days after the completion of the strategy required by subsection (a)—

''(A) the Secretary of Defense shall establish a pilot program under which the Department of Defense, other than the military departments, shall use modern data formats to improve the usability and functionality of information stored or produced in antiquated data formats, including by the automated conversion of such information to modern data formats; and

''(B) each Secretary of a military department shall establish a pilot program under which such military department shall use modern data formats as described in subparagraph (A).

''(2) BRIEFING.—Not later than 180 days after the completion of the strategy required by subsection (a), the Secretary of Defense and the Secretaries of the military departments shall each submit to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the progress of the pilot program established by such Secretary under this subsection, including specific examples of the use of modern data formats under such pilot program to improve the usability and functionality of information stored or produced in antiquated data formats.

''(3) SUNSET.—Each pilot program established under this subsection shall terminate on the date that is five years after the date of the enactment of this Act.

''(c) MILITARY DEPARTMENT DEFINED.—In this section, the term 'military department' has the meaning given such term in section 101(a) of title 10, United States Code.''

UPDATE OF BIOMETRIC POLICY OF DEPARTMENT OF DEFENSE

Pub. L. 118–159, div. A, title XV, §1523, Dec. 23, 2024, 138 Stat. 2142, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2024], the Under Secretary of Defense for Intelligence and Security shall update the policy of the Department of Defense regarding the protection of biometric data.

''(b) ELEMENTS.—The policy updates required by subsection (a) shall include the following:

''(1) Standards for encrypting and protecting data on biometric collection devices.

''(2) A requirement to sanitize biometric data from collection devices and hard drives prior to disposal of the devices and hard drives.

''(3) A requirement that components of the Department maintain records that they have sanitized all data from biometric collection devices when the devices are turned in for disposal.''

REVIEW AND PLAN RELATING TO CYBER RED TEAMS OF DEPARTMENT OF DEFENSE

Pub. L. 118–31, div. A, title XV, § 1507, Dec. 22, 2023, 137 Stat. 540, provided that:

''(a) REVIEW RELATING TO PRIOR JOINT ASSESSMENT.—

''(1) REVIEW REQUIRED.—Not later than 90 days after the date of the enactment of this Act [Dec. 22, 2023], the officials described in subsection (c) shall review, and assess the status of the implementation of, the recommendations set forth by the Secretary of Defense in response to the joint assessment requirement under section 1660 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1771).

''(2) ELEMENTS.—The review under paragraph (1) shall include, with respect to the recommendations specified in such paragraph—

''(A) the timelines associated with each such recommendation, regardless of whether the recommendation is fully implemented or yet to be fully implemented; and

''(B) a description of any impediments to the implementation of such recommendations encountered.

''(b) PLAN REQUIRED.—

''(1) PLAN.—Not later than 180 days after the date of the enactment of this Act, the officials described in subsection (c) shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan, developed taking into account the findings of the review under subsection (a), to ensure cyber red teams of the Department of Defense achieve sufficient capacity and capability to provide services and meet current and projected future demands on a Defense-wide basis. Such plan shall include—

''(A) a description of the funding necessary for such cyber red teams to achieve such capacity and capability;

''(B) a description of any other resources, personnel, infrastructure, or authorities for access to information necessary for such cyber red teams to achieve such capacity and capability (including with respect to the emulation of threats from foreign countries with advanced cyber capabilities, automation, artificial intelligence or machine learning, and data collection and correlation); and

''(C) updated joint service standards and metrics to ensure the training, staffing, and equipping of such cyber red teams at levels necessary to achieve such capacity and capability.

''(2) IMPLEMENTATION.—Not later than one year after the date of enactment of this Act, the Secretary of Defense shall prescribe such regulations and issue such guidance as the Secretary determines necessary to implement the plan developed under subsection (a).

''(c) OFFICIALS DESCRIBED.—The officials described in this subsection are the Principal Cyber Advisor to the Secretary of Defense, the Chief Information Officer of the Department of Defense, the Director of Operational Test and Evaluation, and the Commander of the United States Cyber Command.

''(d) ANNUAL REPORTS.—Not later than January 31, 2025, and not less frequently than annually thereafter until January 31, 2031, the Director of Operational Test and Evaluation shall include in each annual report required under section 139(h) of title 10, United States Code, an update on progress made with respect to the implementation of this section, including the following:

''(1) The results of test and evaluation events, including any resource or capability shortfalls limiting the capacity or capability of cyber red teams of the Department of Defense to meet operational requirements.

''(2) The extent to which operations of such cyber red teams have expanded across the competition continuum, including during cooperation and competition phases, to match adversary positioning and cyber activities.

''(3) A summary of identified categories of common gaps and shortfalls across cyber red teams of the military departments and Defense Agencies (as such terms are defined in section 101 of title 10, United States Code).

''(4) Any identified lessons learned that would affect training or operational employment decisions relating to the cyber red teams of the Department of Defense.''

TRANSFER OF DATA AND TECHNOLOGY DEVELOPED UNDER MOSAICS PROGRAM

Pub. L. 118–31, div. A, title XV, § 1514, Dec. 22, 2023, 137 Stat. 545, provided that:

''(a) TRANSFERS AUTHORIZED.—The Secretary of Defense may transfer to eligible private sector entities data and technology developed under the MOSAICS program to enhance cyber threat detection and protection of critical industrial control system assets used for electricity distribution.

''(b) AGREEMENTS.—In carrying out subsection (a), the Secretary of Defense may—

''(1) enter into cooperative research and development agreements under section 4026 of title 10, United States Code; and

''(2) use such other mechanisms for the transfer of technology and data as are authorized by law.

''(c) [sic; there are two subsecs. (c)] NOTIFICATION.—Not later than 15 days after any date on which the Secretary determines to transfer data or technology to an eligible private sector entity under subsection (a), the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written notification of such determination. Such notification shall include the following:

''(1) An identification of the data or technology to be transferred.

''(2) An identification of the eligible private sector entity, including an identification of the specific individual employed by or otherwise associated with such entity responsible for the security and integrity of the data or technology to be received.

''(3) A detailed description of any special security handling instructions required pursuant to an agreement entered into between the Secretary and the eligible private sector entity for such transfer.

''(4) Timelines associated with such transfer.

''(c) [sic] DEFINITIONS.—In this section:

''(1) The term 'eligible private sector entity' means a private sector entity that—

''(A) has functions relevant to the civil electricity sector; and

''(B) is determined by the Secretary of Defense to be eligible to receive data and technology transferred under subsection (a).

''(2) The term 'MOSAICS program' means the program of the Department of Defense known as the 'More Situational Awareness for Industrial Control Systems Joint Capabilities Technology Demonstration program', or successor program.''

MODERNIZATION PROGRAM FOR NETWORK BOUNDARY AND CROSS-DOMAIN DEFENSE

Pub. L. 118–31, div. A, title XV, § 1515, Dec. 22, 2023, 137 Stat. 546, provided that:

''(a) MODERNIZATION PROGRAM REQUIRED.—The Secretary of Defense shall carry out a modernization program for network boundary and cross-domain defense against cyber attacks. In carrying out such modernization program, the Secretary shall expand upon the fiscal year 2023 pilot program on modernized network boundary defense capabilities and the initial deployment of such capabilities to the primary Internet access points of the Department of Defense managed by the Director of the Defense Information Systems Agency.

''(b) PROGRAM PHASES.—

''(1) IN GENERAL.—The Secretary of Defense shall implement the modernization program under subsection (a) in phases, with the objective of completing such program by October 1, 2028.

''(2) OBJECTIVES.—The phases required by paragraph (1) shall include the following objectives:

''(A) By September 30, 2026, completion of—

''(i) the pilot program specified in subsection (a) and the deployment of modernized network boundary defense capabilities to the Internet access points managed by the Director of the Defense Information Systems Agency; and

''(ii) the extension of modernized network boundary defense capabilities to all additional Internet access points of the information network of the Department of Defense.

''(B) By September 30, 2027, the conduct of a survey, completion of a pilot program, and deployment of modernized network boundary defense capabilities to the access points and cross-domain capabilities of the Secret Internet Protocol Router Network.

''(C) By September 30, 2028, the conduct of a survey, completion of a pilot program, and deployment of modernized network boundary defense capabilities to any remaining classified network or enclave of the information network of the Department.

''(c) IMPLEMENTATION PLAN.—Not later than 90 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for the implementation of the modernization program under subsection (a). Such plan shall include—

''(1) a summary of findings from the pilot program specified in subsection (a); and

''(2) an identification of the resources necessary for such implementation, including for implementing the phase of the modernization program specified in subsection (b)(2)(C).''

ESTABLISHMENT OF CERTAIN IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT ACTIVITIES AS PROGRAM OF RECORD

Pub. L. 118–31, div. A, title XV, § 1516, Dec. 22, 2023, 137 Stat. 546, provided that:

''(a) ESTABLISHMENT OF PROGRAM OF RECORD.—

''(1) PROGRAM OF RECORD.—Except as provided in subsection (b), not later than 120 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall establish a program of record, governed by standard Department of Defense requirements and practices, and transition all covered activities to such program of record.

''(2) OBJECTIVES.—The program of record under subsection (a) shall include, at a minimum, covered activities undertaken to achieve the following objectives:

''(A) Correcting weaknesses in authentication and credentialing security, including with respect to the program of the Department of Defense known as the 'Public Key Infrastructure' program (or any successor program), identified by the Director of Operational Test and Evaluation in a report submitted to Congress in April, 2023, titled 'FY14–21 Observations of the Compromise of Cyber Credentials'.

''(B) Implementing improved authentication technologies, such as biometric and behavioral authentication techniques and other non-password-based solutions.

''(3) BRIEFING.—Not later than 150 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the covered activities to be included under the program of record under subsection (a).

''(b) WAIVER AUTHORITY.—

''(1) AUTHORITY.—The Secretary of Defense may waive the requirement under subsection (a) if the Secretary of Defense determines that the objectives listed in paragraph (2) of such subsection would be better achieved, and the level of rigor of the operational testing and oversight requirements applicable to such objectives would be improved, through a management approach other than the establishment of a program of record and transition of covered activities to such program of record.

''(2) JUSTIFICATION.—Not later than 14 days after issuing a waiver under paragraph (1), the Secretary of Defense shall submit to the congressional defense committees a detailed justification for the waiver, including—

''(A) an explanation of why the establishment of a program of record is not the preferred approach to achieve the objectives listed in subsection (a)(2);

''(B) details relating to the management approach proposed to be implemented in lieu of the establishment of a program of record;

''(C) an implementation plan for such proposed alternative approach; and

''(D) such other information as the Secretary of Defense determines appropriate.

''(c) DESIGNATION OF DATA ATTRIBUTES.—Not later than 120 days after the date of the enactment of this Act, the Chief Information Officer of the Department of Defense, in coordination with the Secretaries of the military departments, shall complete the designation of Tier 1 level data attributes to be used as a baseline set of standardized attributes for identity, credential, and access management, Defense-wide.

''(d) BRIEFING.—Upon completing the requirement under subsection (c), the Chief Information Officer of the Department of Defense and the Secretaries of the military departments shall provide to the Committees on Armed Services of the House of Representatives and the Senate a briefing on the activities carried out under this section.

''(e) DEFINITIONS.—In this section:

''(1) The term 'covered activity' means any activity of the Office of the Secretary of Defense or a Defense Agency relating to the identity, credential, and access management initiative of the Department of Defense.

''(2) The term 'Defense Agency' has the meaning given that term in section 101 of title 10, United States Code.''

PILOT PROGRAM ON ASSURING CRITICAL INFRASTRUCTURE SUPPORT FOR MILITARY CONTINGENCIES

Pub. L. 118–31, div. A, title XV, § 1517, Dec. 22, 2023, 137 Stat. 548, provided that:

''(a) ESTABLISHMENT OF PILOT PROGRAM.—Not later than 60 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall establish a pilot program to be known as the 'Assuring Critical Infrastructure Support for Military Contingencies Pilot Program'.

''(b) SELECTION OF INSTALLATIONS.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, shall select not fewer than four geographically diverse military installations at which to carry out the pilot program under subsection (a).

''(2) PRIORITIZATION.—

''(A) IN GENERAL.—In selecting military installations under paragraph (1), the Secretary of Defense shall give priority to any military installation that the Secretary determines is a key component of not fewer than two contingency plans or operational plans, with further priority given to such plans in the area of responsibility of the United States Indo-Pacific Command or the United States European Command.

''(B) SELECTION BETWEEN EQUAL PRIORITIES.—If two or more military installations qualify for equal

priority under subparagraph (A), the Secretary of Defense shall give further priority for selection under such paragraph to any such military installation that the Secretary of Defense determines is—

''(i) connected to national-level infrastructure;

''(ii) located near a commercial port; or

''(iii) located near a national financial hub.

''(c) ACTIVITIES.—In carrying out the pilot program under subsection (a), the Secretary of Defense, acting through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, shall—

''(1) without duplicating or disrupting existing cyber exercise activities under the National Cyber Exercise Program under section 2220B of the Homeland Security Act of 2002 (6 U.S.C. 665h), conduct cyber resiliency and reconstitution stress test scenarios through tabletop exercises and, if possible, live exercises—

''(A) to assess how to prioritize restoration of power, water, and telecommunications for a military installation in the event of a significant cyberattack on regional critical infrastructure that has similar impacts on State and local infrastructure; and

''(B) to determine the recovery process needed to ensure the military installation has the capability to function and support an overseas contingency operation or a homeland defense mission, as appropriate;

''(2) map dependencies on power, water, and telecommunications at the military installation and the connections to distribution and generation outside the military installation;

''(3) recommend priorities for the order of recovery for the military installation in the event of a significant cyberattack, considering both the requirements needed for operations of the military installation and the potential participation of personnel at the military installation in an overseas contingency operation or a homeland defense mission; and

''(4) develop a lessons-learned database from the exercises conducted under paragraph (1) across all military installations participating in the pilot program, to be shared with the Committees on Armed Services of the House of Representatives and the Senate.

''(d) COORDINATION WITH RELATED PROGRAMS.—The Secretary of Defense, acting through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, shall ensure that activities under subsection (c) are coordinated with—

''(1) private entities that operate power, water, and telecommunications for a military installation participating in the pilot program under subsection (a);

''(2) relevant military and civilian personnel; and

''(3) any other entity that the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs determines is relevant to the execution of activities under subsection (c).

''(e) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the Assistant to the President for Homeland Security, the National Cyber Director, the head of any other relevant Sector Risk Management Agency, the Committees on Armed Services of the House of Representatives and the Senate, and, if the Secretary of Defense determines it appropriate, relevant private sector owners and operators of critical infrastructure a report on the activities carried out under pilot program under subsection (a), including a description of any operational challenges identified.

''(f) DEFINITIONS.—In this section:

''(1) The term 'critical infrastructure' has the meaning given that term in the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c).

''(2) The term 'Sector Risk Management Agency' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).''

REQUIREMENTS FOR IMPLEMENTATION OF USER ACTIVITY MONITORING FOR CERTAIN PERSONNEL

Pub. L. 118–31, div. A, title XV, §1537, Dec. 22, 2023, 137 Stat. 570, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall require each head of a component of the Department of Defense to fully implement each directive, policy, and program requirement for user activity monitoring and least privilege access controls with respect to the personnel of that component, including Federal employees and contractors, granted access to classified information and classified networks, including the following directives (and any successor directives):

''(1) The Committee on National Security Systems Directive 504, issued on February 4, 2014, relating to the protection of national security systems from insider threats (including any annex to such directive).

''(2) Department of Defense Directive 5205.16, issued on September 30, 2014, relating to the insider threat program of the Department of Defense.

''(b) ADDITIONAL REQUIREMENT.—The Secretary of Defense shall require each head of a component of the Department of Defense to implement, with respect to systems, devices, and personnel of the component, automated controls to detect and prohibit privileged user accounts from performing general user activities not requiring privileged access.

''(c) PERIODIC TESTING.—The Secretary shall require that, not less frequently than once every two years, each head of a component of the Department of Defense—

''(1) conducts insider threat testing using threat-realistic tactics, techniques, and procedures; and

''(2) submits to the Under Secretary of Defense for Intelligence and Security, the Chief Information Officer of the Department of Defense, and the Director of Operational Test and Evaluation of the Department of Defense a report on the findings of the head with respect to the testing conducted pursuant to paragraph (1).

''(d) REPORT.—Not later than 180 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of Defense shall submit to the appropriate congressional committees a report on the implementation of this section.

''(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

''(1) the Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives; and

''(2) the Committee on Armed Services and the Select Committee on Intelligence of the Senate.''

MANAGEMENT BY DEPARTMENT OF DEFENSE OF MOBILE APPLICATIONS

Pub. L. 118–31, div. A, title XV, §1552, Dec. 22, 2023, 137 Stat. 579, provided that:

''(a) IMPLEMENTATION OF RECOMMENDATIONS.—

''(1) IN GENERAL.—The Secretary of Defense shall evaluate and implement to the maximum extent practicable the recommendations of the Inspector General of the Department of Defense with respect to managing mobile applications contained in the report set forth by the Inspector General dated February 9, 2023, and titled 'Management Advisory: The DoD's Use of Mobile Applications' (Report No. DODIG–2023–041).

''(2) DEADLINE.—The Secretary shall implement each of the recommendations specified in subsection (a) by not later than one year after the date of the enactment of this Act [Dec. 22, 2023] unless the Secretary submits to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a written notification of any specific recommendation that the Secretary declines to implement or plans to implement after the date that is one year after the date of the enactment of this Act.

''(b) BRIEFING ON REQUIREMENTS RELATED TO COVERED APPLICATIONS.—

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary shall provide to the congressional defense committees a

briefing on actions taken by the Secretary to enforce compliance with existing policy of the Department of Defense that prohibits—

''(A) the installation and use of covered applications on Federal Government devices; and

''(B) the use of covered applications on the Department of Defense Information Network on personal devices.

''(2) COVERED APPLICATIONS DEFINED.—In this subsection, the term 'covered applications' means the social networking service TikTok, or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.''

ACTIONS TO ADDRESS SERIOUS DEFICIENCIES IN ELECTRONIC PROTECTION OF SYSTEMS THAT OPERATE IN THE RADIO FREQUENCY SPECTRUM

Pub. L. 118–31, div. A, title XVI, § 1686, Dec. 22, 2023, 137 Stat. 620, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall—

''(1) establish requirements for and assign sufficient priority to ensuring electronic protection of military sensor, navigation, and communications systems and subsystems against jamming, spoofing, and unintended interference from military systems of the United States and foreign adversaries; and

''(2) provide management oversight and supervision of the military departments to ensure military systems that emit and receive radio frequencies are protected against threats and interference from United States and foreign adversary military systems operating in the same or adjacent radio frequencies.

''(b) SPECIFIC REQUIRED ACTIONS.—The Secretary of Defense shall require the military departments and combat support agencies to carry out the following activities:

''(1) Not later than 270 days after the date of the enactment of this Act [Dec. 22, 2023], develop and approve requirements, through the Joint Requirements Oversight Council as appropriate, for every radar, signals intelligence, navigation, and communications system and subsystem subject to the Global Force Management process to ensure such systems and subsystems are able to withstand threat-realistic levels of jamming, spoofing, and unintended interference, including self-generated interference.

''(2) Not less frequently than once every 4 years, test each system and subsystem described in paragraph (1) at a test range that permits threat-realistic electronic warfare attacks against the system or subsystem by a red team or simulated opposition force, with the first set of highest priority systems to be initially tested by not later than the end of fiscal year 2025.

''(3) With respect to each system and subsystem described in paragraph (1) that fails to meet electronic protection requirements during testing conducted under paragraph (2)—

''(A) not later than 3 years after the initial failed test, retrofit the system or subsystem with electronic protection measures that can withstand threat-realistic jamming, spoofing, and unintended interference; and

''(B) not later than 4 years after the initial failed test, retest such systems and subsystems.

''(4) Survey, identify, and test available technology that can be practically and affordably retrofitted on the systems and subsystems described in paragraph (1) and which provides robust protection against threat-realistic jamming, spoofing, and unintended interference.

''(5) Design and build electronic protection into ongoing and future development programs to withstand expected jamming and spoofing threats and unintended interference.

''(c) WAIVER.—The Secretary of Defense may establish a process for issuing waivers, on a case-by-case basis, for the testing requirement under paragraph (2) of subsection (b) and for the retrofit requirement under paragraph (3) of such subsection.

''(d) ANNUAL REPORTS.—Concurrent with the submission of the budget of the President to Congress pursuant to section 1105(a) of title 31, United States Code, for each of fiscal years 2025 through 2030, the Director of Operational Test and Evaluation shall submit to the Electronic Warfare Executive Committee of the Department of Defense and the Committees on Armed Services of the Senate and the House of Representatives a comprehensive annual report that—

''(1) aggregates and summarizes information received from the military departments and combat support agencies for purposes of the preparation of the report; and

''(2) includes a description of—

''(A) the activities carried out to implement the requirements of this section;

''(B) the systems and subsystems subject to testing in the previous year and the results of such tests, including a description of the requirements for electronic protection established for the tested systems and subsystems; and

''(C) each waiver issued in the previous year with respect to such requirements, together with a detailed rationale for the waiver and a plan for addressing any issues that formed the basis of the waiver request.''

OPERATIONAL TESTING FOR COMMERCIAL CYBERSECURITY CAPABILITIES

Pub. L. 117–263, div. A, title XV, § 1514, Dec. 23, 2022, 136 Stat. 2895, provided that:

''(a) DEVELOPMENT AND SUBMISSION OF PLANS.—Not later than February 1, 2024, the Chief Information Officer of the Department of Defense and the Chief Information Officers of the military departments shall develop and submit plans described in subsection (b) to the Director of Operational Test and Evaluation who may approve the implementation of the plans pursuant to subsection (c).

''(b) PLANS DESCRIBED.—The plans described in this subsection are plans that—

''(1) ensure covered cybersecurity capabilities are appropriately tested, evaluated, and proven operationally effective, suitable, and survivable prior to operation on a Department of Defense network; and

''(2) specify how test results will be expeditiously provided to the Director of Operational Test and Evaluation.

''(c) ASSESSMENT.—In reviewing the plans submitted under subsection (a), the Director of Operational Test and Evaluation shall conduct an assessment that includes consideration of the following:

''(1) Threat-realistic operational testing, including representative environments, variation of operational conditions, and inclusion of a realistic opposing force.

''(2) The use of Department of Defense cyber red teams, as well as any enabling contract language required to permit threat-representative red team assessments.

''(3) Collaboration with the personnel using the commercial cybersecurity capability regarding the results of the testing to improve operators' ability to recognize and defend against cyberattacks.

''(4) The extent to which additional resources may be needed to remediate any shortfalls in capability to make the commercial cybersecurity capability effective, suitable, and cyber survivable in an operational environment of the Department.

''(5) Identification of training requirements, and changes to training, sustainment practices, or concepts of operation or employment that may be needed to ensure the effectiveness, suitability, and cyber survivability of the commercial cybersecurity capability.

''(d) POLICIES AND REGULATIONS.—Not later than February 1, 2024, the Secretary of Defense shall issue such policies and guidance and prescribe such regulations as the Secretary determines necessary to carry out this section.

''(e) REPORTS.—Not later than January 31, 2025, and not less frequently than annually thereafter until January 31, 2030, the Director shall include in each annual report required by section 139(h) of title 10, United States Code, the following:

''(1) The status of the plans developed under subsection (a).

''(2) The number and type of test and evaluation events completed in the past year for such plans, disaggregated by component of the Department, and including resources devoted to each event.

''(3) The results from such test and evaluation events, including any resource shortfalls affecting the number of commercial cybersecurity capabilities that could be assessed.

''(4) A summary of identified categories of common gaps and shortfalls found during testing.

''(5) The extent to which entities responsible for developing and testing commercial cybersecurity capabilities have responded to recommendations made by the Director in an effort to gain favorable determinations.

''(6) Any identified lessons learned that would impact training, sustainment, or concepts of operation or employment decisions relating to the assessed commercial cybersecurity capabilities.

''(f) DEFINITION.—In this section, the term 'covered cybersecurity capabilities' means any of the following:

''(1) Commercial products (as defined in section 103 of title 41, United States Code) acquired and deployed by the Department of Defense to satisfy the cybersecurity requirements of one or more Department components.

''(2) Commercially available off-the-shelf items (as defined in section 104 of title 41, United States Code) acquired and deployed by the Department of Defense to satisfy the cybersecurity requirements of one or more Department components.

''(3) Noncommercial items acquired through the Adaptive Acquisition Framework and deployed by the Department of Defense to satisfy the cybersecurity requirements of one or more Department components.''

PLAN FOR COMMERCIAL CLOUD TEST AND EVALUATION

Pub. L. 117–263, div. A, title XV, §1553, Dec. 23, 2022, 136 Stat. 2920, provided that:

''(a) POLICY AND PLAN.—Not later than 180 days after the date of enactment of this Act [Dec. 23, 2022], the Secretary of Defense, in consultation with commercial industry, shall implement a policy and plan for test and evaluation of the cybersecurity of the clouds of commercial cloud service providers that provide, or are intended to provide, storage or computing of classified data of the Department of Defense.

''(b) CONTENTS.—The policy and plan under subsection (a) shall include the following:

''(1) A requirement that, beginning on the date of the enactment of this Act, future contracts with cloud service providers for storage or computing of classified data of the Department include provisions that permit the Secretary to conduct independent, threat-realistic assessments of the commercial cloud infrastructure, including with respect to—

''(A) the storage, compute, and enabling elements, including the control plane and virtualization hypervisor for mission elements of the Department supported by the cloud provider; and

''(B) the supporting systems used in the fulfillment, facilitation, or operations relating to the mission of the Department under the contract, including the interfaces with these systems.

''(2) An explanation as to how the Secretary intends to proceed on amending existing contracts with cloud service providers to permit the same level of assessments required for future contracts under paragraph (1).

''(3) Identification and description of any proposed tiered test and evaluation requirements aligned with different impact and classification levels.

''(c) WAIVER AUTHORITY.—The Secretary may include in the policy and plan under subsection (a) an authority to waive any requirement under subsection (b) if the waiver is jointly approved by the Chief Information Officer of the Department of Defense and the Director of Operational Test and Evaluation.

''(d) SUBMISSION.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit to the Committees on Armed Services of the Senate and the House of Representatives the policy and plan under subsection (a).

''(e) THREAT-REALISTIC ASSESSMENT DEFINED.—In this section, the term 'threat-realistic assessments' means, with respect to commercial cloud infrastructure, activities that—

''(1) are designed to accurately emulate cyber threats from advanced nation state adversaries, such as Russia and China; and

''(2) include cooperative penetration testing and no-notice threat-emulation activities where personnel of the Department of Defense attempt to penetrate and gain control of the cloud-provider facilities, networks, systems, and defenses associated with, or which enable, the supported missions of the Department.''

ASSESSMENTS OF WEAPONS SYSTEMS VULNERABILITIES TO RADIO-FREQUENCY ENABLED CYBER ATTACKS

Pub. L. 117–263, div. A, title XV, §1559, Dec. 23, 2022, 136 Stat. 2926, as amended by Pub. L. 118–31, div. A, title XV, §1502(a)(2)(F), Dec. 22, 2023, 137 Stat. 538, provided that:

''(a) ASSESSMENTS.—The Secretary of Defense shall ensure that the activities required by and conducted pursuant to section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1118) [10 U.S.C. 2224 note] and the amendments made by section 1712 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 134 Stat. 4087 [amending section 1647 of Pub. L. 114–92, set out as a note under this section, and section 1640 of Pub. L. 115–91, formerly set out as a note under this section]) include regular assessments of the vulnerabilities to and mission risks presented by radio-frequency enabled cyber attacks with respect to the operational technology embedded in weapons systems, aircraft, ships, ground vehicles, space systems, sensors, and datalink networks of the Department of Defense.

''(b) ELEMENTS.—The assessments under subsection (a) with respect to vulnerabilities and risks described in such subsection shall include—

''(1) identification of such vulnerabilities and risks;

''(2) ranking of vulnerability, severity, and priority;

''(3) development and selection of options, with associated costs and schedule, to correct such vulnerabilities, including installation of intrusion detection capabilities;

''(4) an evaluation of the cybersecurity sufficiency for Military Standard 1553; and

''(5) development of integrated risk-based plans to implement the corrective actions selected.

''(c) DEVELOPMENT OF CORRECTIVE ACTIONS.—In developing corrective actions under subsection (b)(3), the assessments under subsection (a) shall—

''(1) consider the missions supported by the assessed weapons systems, aircraft, ships, ground vehicles, space systems, sensors, or datalink networks, as the case may be, to ensure that the corrective actions focus on the vulnerabilities that create the greatest risks to the missions;

''(2) be shared and coordinated with the principal staff assistant with primary responsibility for the strategic cybersecurity program; and

''(3) address requirements for deployed and nondeployed members of the Armed Forces to analyze data collected on the weapons systems and respond to attacks.

''(d) INTELLIGENCE INFORMED ASSESSMENTS.—The assessments under subsection (a) shall be informed by in-

telligence, if available, and technical judgment regarding potential threats to embedded operational technology during operations of the Armed Forces.

''(e) COORDINATION.—

''(1) COORDINATION AND INTEGRATION OF ACTIVITIES.—The assessments under subsection (a) shall be fully coordinated and integrated with activities described in such subsection.

''(2) COORDINATION OF ORGANIZATIONS.—The Secretary shall ensure that the organizations conducting the assessments under subsection (a) in the military departments, the United States Special Operations Command, and the Defense Agencies coordinate with each other and share best practices, vulnerability analyses, and technical solutions with the principal staff assistant with primary responsibility for the Strategic Cybersecurity Program.''

COORDINATION BETWEEN UNITED STATES CYBER COMMAND AND PRIVATE SECTOR

Pub. L. 117–81, div. A, title XV, § 1508, Dec. 27, 2021, 135 Stat. 2032, provided that:

''(a) VOLUNTARY PROCESS.—Not later than January 1, 2023, the Commander of United States Cyber Command shall establish a voluntary process to engage with private sector information technology and cybersecurity entities to explore and develop methods and plans through which the capabilities, knowledge, and actions of—

''(1) private sector entities operating inside the United States to defend against foreign malicious cyber actors could assist, or be coordinated with, the actions of United States Cyber Command operating outside the United States against such foreign malicious cyber actors; and

''(2) United States Cyber Command operating outside the United States against foreign malicious cyber actors could assist, or be coordinated with, the actions of private sector entities operating inside the United States against such foreign malicious cyber actors.

''(b) ANNUAL BRIEFING.—

''(1) IN GENERAL.—During the period beginning on March 1, 2022, and ending on March 1, 2026, the Commander of United States Cyber Command shall, not less frequently than once each year, provide to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a briefing on the status of any activities conducted pursuant to subsection (a).

''(2) ELEMENTS.—Each briefing provided under paragraph (1) shall include the following:

''(A) Such recommendations for legislative or administrative action as the Commander of United States Cyber Command considers appropriate to improve and facilitate the exploration and development of methods and plans under subsection (a).

''(B) Such recommendations as the Commander may have for increasing private sector participation in such exploration and development.

''(C) A description of the challenges encountered in carrying out subsection (a), including any concerns expressed to the Commander by private sector partners regarding participation in such exploration and development.

''(D) Information relating to how such exploration and development with the private sector could assist military planning by United States Cyber Command.

''(E) Such other matters as the Commander considers appropriate.

''(c) CONSULTATION.—In developing the process described in subsection (a), the Commander of United States Cyber Command shall consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and the heads of any other Federal agencies the Commander considers appropriate.

''(d) INTEGRATION WITH OTHER EFFORTS.—The Commander of United States Cyber Command shall ensure that the process described in subsection (a) makes use of, builds upon, and, as appropriate, integrates with and does not duplicate, other efforts of the Department of Homeland Security and the Department of Defense relating to cybersecurity, including the following:

''(1) The Joint Cyber Defense Collaborative of the Cybersecurity and Infrastructure Security Agency.

''(2) The Cybersecurity Collaboration Center and Enduring Security Framework of the National Security Agency.

''(3) The office for joint cyber planning of the Department of Homeland Security.

''(e) PROTECTION OF TRADE SECRETS AND PROPRIETARY INFORMATION.—The Commander of United States Cyber Command shall ensure that any trade secret or proprietary information of a private sector entity engaged with the Department of Defense through the process established under subsection (a) that is made known to the Department pursuant to such process remains private and protected unless otherwise explicitly authorized by such entity.

''(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize United States Cyber Command to conduct operations inside the United States or for private sector entities to conduct offensive cyber activities outside the United States, except to the extent such operations or activities are permitted by a provision of law in effect on the day before the date of the enactment of this Act [Dec. 27, 2021].''

ENTERPRISE-WIDE PROCUREMENT OF CYBER DATA PRODUCTS AND SERVICES

Pub. L. 117–81, div. A, title XV, § 1521, Dec. 27, 2021, 135 Stat. 2040, as amended by Pub. L. 118–31, div. A, title XV, § 1522, Dec. 22, 2023, 137 Stat. 553; Pub. L. 118–159, div. A, title XV, § 1501, Dec. 23, 2024, 138 Stat. 2131, provided that:

''(a) PROGRAM.—Not later than one year after the date of the enactment of this Act [Dec. 27, 2021], the Secretary of Defense shall designate an executive agent for Department of Defense-wide procurement of cyber data products and services. The executive agent shall establish a program management office responsible for such procurement, and the program manager of such program office shall be responsible for the following:

''(1) Surveying components of the Department for the cyber data products and services needs of such components.

''(2) Conducting market research of cyber data products and services.

''(3) Developing or facilitating development of requirements, both independently and through consultation with components, for the acquisition of cyber data products and services.

''(4) Developing and instituting model contract language for the acquisition of cyber data products and services, including contract language that facilitates components' requirements for ingesting, sharing, using and reusing, structuring, and analyzing data derived from such products and services.

''(5) Conducting procurement of cyber data products and services on behalf of the Department of Defense, including negotiating contracts with a fixed number of licenses based on aggregate component demand and negotiation of extensible contracts.

''(6) Evaluating emerging cyber technologies, such as artificial intelligence-enabled security tools, for efficacy and applicability to the requirements of the Department of Defense.

''(7) Carrying out the responsibilities specified in paragraphs (1) through (6) with respect to the cyber data products and services needs of the Cyberspace Operations Forces, such as cyber data products and services germane to cyberspace topology and identification of adversary threat activity and infrastructure, including—

''(A) facilitating the development of cyber data products and services requirements for the Cyberspace Operations Forces, conducting market research regarding the future cyber data products and

services needs of the Cyberspace Operations Forces, and conducting acquisitions pursuant to such requirements and market research;

''(B) coordinating cyber data products and services acquisition and management activities with Joint Cyber Warfighting Architecture acquisition and management activities, including activities germane to data storage, data management, and development of analytics;

''(C) implementing relevant Department of Defense and United States Cyber Command policy germane to acquisition of cyber data products and services;

''(D) leading or informing the integration of relevant datasets and services, including Government-produced threat data, commercial cyber threat information, collateral telemetry data, topology-relevant data, sensor data, and partner-provided data; and

''(E) facilitating the development of tradecraft and operational workflows based on relevant cyber data products and services.

''(b) COORDINATION.—In implementing this section, each component of the Department of Defense shall coordinate its cyber data products and services requirements and potential procurement plans relating to such products and services with the program management office established pursuant to subsection (a) so as to enable such office to determine if satisfying such requirements or procurement of such products and services on an enterprise-wide basis would serve the best interests of the Department.

''(c) PROHIBITION.—Beginning not later than 540 days after the date of the enactment of this Act, no component of the Department of Defense may independently procure a cyber data product or service that has been procured by the program management office established pursuant to subsection (a), unless—

''(1) such component is able to procure such product or service at a lower per-unit price than that available through such office;

''(2) such office has approved such independent purchase; or

''(3) such component submits to such office a justification for such component to independently procure such product or service that such component determines as demonstrating—

''(A) the compelling need for such product or service; and

''(B) either the urgency for such product or service or the need to ensure competition in the market for such product or service supports such independent procurement by such component.

''(d) EXCEPTION.—United States Cyber Command and the National Security Agency may conduct joint procurements of products and services, including cyber data products and services, except that the requirements of subsections (b) and (c) shall not apply to the National Security Agency.

''(e) DEFINITION.—In this section, the term 'cyber data products and services' means commercially-available datasets and analytic services germane to offensive cyber, defensive cyber, and DODIN operations, including products and services that provide technical data, indicators, and analytic services relating to the targets, infrastructure, tools, and tactics, techniques, and procedures of cyber threats.''

PROTECTIVE DOMAIN NAME SYSTEM WITHIN THE DEPARTMENT OF DEFENSE

Pub. L. 117–81, div. A, title XV, §1524, Dec. 27, 2021, 135 Stat. 2042, provided that:

''(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Dec. 27, 2021], the Secretary of Defense shall ensure each component of the Department of Defense uses a Protective Domain Name System (PDNS) instantiation offered by the Department.

''(b) EXEMPTIONS.—The Secretary of Defense may exempt a component of the Department from using a PDNS instantiation for any reason except with respect to cost or technical application.

''(c) REPORT TO CONGRESS.—Not later than 150 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that includes information relating to—

''(1) each component of the Department of Defense that uses a PDNS instantiation offered by the Department;

''(2) each component exempt from using a PDNS instantiation pursuant to subsection (b); and

''(3) efforts to ensure that each PDNS instantiation offered by the Department connects and shares relevant and timely data.''

CYBER DATA MANAGEMENT

Pub. L. 117–81, div. A, title XV, §1527, Dec. 27, 2021, 135 Stat. 2043, provided that:

''(a) IN GENERAL.—The Commander of United States Cyber Command and the Secretaries of the military departments, in coordination with the Principal Cyber Advisor to the Secretary, the Chief Information Officer and the Chief Data Officer of the Department of Defense, and the Chairman of the Joint Chiefs of Staff, shall—

''(1) access, acquire, and use mission-relevant data to support offensive cyber, defensive cyber, and DODIN operations from the intelligence community, other elements of the Department of Defense, and the private sector;

''(2) develop policy, processes, and operating procedures governing the access, ingest, structure, storage, analysis, and combination of mission-relevant data, including—

''(A) intelligence data;

''(B) internet traffic, topology, and activity data;

''(C) cyber threat information;

''(D) Department of Defense Information Network sensor, tool, routing infrastructure, and endpoint data; and

''(E) other data management and analytic platforms pertinent to United States Cyber Command missions that align with the principles of Joint All Domain Command and Control;

''(3) pilot efforts to develop operational workflows and tactics, techniques, and procedures for the operational use of mission-relevant data by the Cyberspace Operations Forces; and

''(4) evaluate data management platforms used to carry out paragraphs (1), (2), and (3) to ensure such platforms operate consistently with the Deputy Secretary of Defense's Data Decrees signed on May 5, 2021.

''(b) ROLES AND RESPONSIBILITIES.—

''(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 27, 2021], the Commander of United States Cyber Command and the Secretaries of the military departments, in coordination with the Principal Cyber Advisor to the Secretary, the Chief Information Officer and Chief Data Officer of the Department of Defense, and the Chairman of the Joint Chiefs of Staff, shall establish the specific roles and responsibilities of the following in implementing each of the tasks required under subsection (a):

''(A) United States Cyber Command.

''(B) Program offices responsible for the components of the Joint Cyber Warfighting Architecture.

''(C) The military services.

''(D) Entities in the Office of the Secretary of Defense.

''(E) Any other program office, headquarters element, or operational component newly instantiated or determined relevant by the Secretary.

''(2) BRIEFING.—Not later than 300 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense

committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the roles and responsibilities established under paragraph (1).''

ZERO TRUST STRATEGY, PRINCIPLES, MODEL ARCHITECTURE, AND IMPLEMENTATION PLANS

Pub. L. 118–159, div. A, title XV, § 1513, Dec. 23, 2024, 138 Stat. 2136, provided that:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2024], the Chief Information Officer of the Department of Defense shall develop guidance for how—

''(1) the zero trust strategy of the Department of Defense developed under section 1528 of the National Defense Authorization Act for Fiscal Year 2022 (10 U.S.C. 2224 note) [set out below] applies to Internet of Things hardware, including human-wearable devices, sensors, and other smart technology used by the United States in military operations; and

''(2) the role identity, credential, and access management technologies serve in enforcing such zero trust strategy.

''(b) INTERNET OF THINGS DEFINED.—In this section, the term 'Internet of Things' has the meaning given such term by the National Institution of Standards and Technology in NIST Special Publication 800-172 and any amendatory or superseding document relating thereto.''

Pub. L. 117–81, div. A, title XV, § 1528, Dec. 27, 2021, 135 Stat. 2044, as amended by Pub. L. 117–263, div. A, title XV, § 1501(c)(2), Dec. 23, 2022, 136 Stat. 2879, provided that:

''(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 27, 2021], the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall jointly develop a zero trust strategy, principles, and a model architecture to be implemented across the Department of Defense Information Network, including classified networks, operational technology, and weapon systems.

''(b) STRATEGY, PRINCIPLES, AND MODEL ARCHITECTURE ELEMENTS.—The zero trust strategy, principles, and model architecture required under subsection (a) shall include, at a minimum, the following elements:

''(1) Prioritized policies and procedures for establishing implementations of mature zero trust enabling capabilities within on-premises, hybrid, and pure cloud environments, including access control policies that determine which persona or device shall have access to which resources and the following:

''(A) Identity, credential, and access management.

''(B) Macro and micro network segmentation, whether in virtual, logical, or physical environments.

''(C) Traffic inspection.

''(D) Application security and containment.

''(E) Transmission, ingest, storage, and real-time analysis of cybersecurity metadata endpoints, networks, and storage devices.

''(F) Data management, data rights management, and access controls.

''(G) End-to-end encryption.

''(H) User access and behavioral monitoring, logging, and analysis.

''(I) Data loss detection and prevention methodologies.

''(J) Least privilege, including system or network administrator privileges.

''(K) Endpoint cybersecurity, including secure host, endpoint detection and response, and comply-to-connect requirements.

''(L) Automation and orchestration.

''(M) Configuration management of virtual machines, devices, servers, routers, and similar to be maintained on a single virtual device approved list (VDL).

''(2) Policies specific to operational technology, critical data, infrastructures, weapon systems, and classified networks.

''(3) Specification of enterprise-wide acquisitions of capabilities conducted or to be conducted pursuant to the policies referred to in paragraph (2).

''(4) Specification of standard zero trust principles supporting reference architectures and metrics-based assessment plan.

''(5) Roles, responsibilities, functions, and operational workflows of zero trust cybersecurity architecture and information technology personnel—

''(A) at combatant commands, military services, and defense agencies; and

''(B) Joint Forces Headquarters-Department of Defense Information Network.

''(c) ARCHITECTURE DEVELOPMENT AND IMPLEMENTATION.—In developing and implementing the zero trust strategy, principles, and model architecture required under subsection (a), the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall—

''(1) coordinate with—

''(A) the Principal Cyber Advisor to the Secretary of Defense;

''(B) the Director of the National Security Agency Cybersecurity Directorate;

''(C) the Director of the Defense Advanced Research Projects Agency;

''(D) the Chief Information Officer of each military service;

''(E) the Commanders of the cyber components of the military services;

''(F) the Principal Cyber Advisor of each military service;

''(G) the Chairman of the Joints Chiefs of Staff; and

''(H) any other component of the Department of Defense as determined by the Chief Information Officer and the Commander;

''(2) assess the utility of the Joint Regional Security Stacks, automated continuous endpoint monitoring program, assured compliance assessment solution, and each of the defenses at the Internet Access Points for their relevance and applicability to the zero trust architecture and opportunities for integration or divestment;

''(3) employ all available resources, including online training, leveraging commercially available zero trust training material, and other Federal agency training, where feasible, to implement cybersecurity training on zero trust at the—

''(A) executive level;

''(B) cybersecurity professional or implementer level; and

''(C) general knowledge levels for Department of Defense users;

''(4) facilitate cyber protection team and cybersecurity service provider threat hunting and discovery of novel adversary activity;

''(5) assess and implement means to effect Joint Force Headquarters-Department of Defense Information Network's automated command and control of the entire Department of Defense Information Network;

''(6) assess the potential of and, as appropriate, encourage, use of third-party cybersecurity-as-a-service models;

''(7) engage with and conduct outreach to industry, academia, international partners, and other departments and agencies of the Federal Government on issues relating to deployment of zero trust architectures;

''(8) assess the current Comply-to-Connect Plan; and

''(9) review past and conduct additional pilots to guide development, including—

''(A) utilization of networks designated for testing and accreditation under section 1658 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 10 U.S.C. 2224 note) [set out below];

''(B) use of automated red team products for assessment of pilot architectures; and

''(C) accreditation of piloted cybersecurity products for enterprise use in accordance with the findings on enterprise accreditation standards conducted pursuant to section 1654 of such Act (Public Law 116–92) [133 Stat. 1764].

''(d) IMPLEMENTATION PLANS.—

''(1) IN GENERAL.—Not later than one year after the finalization of the zero trust strategy, principles, and model architecture required under subsection (a), the head of each military department and the head of each component of the Department of Defense shall transmit to the Chief Information Officer of the Department and the Commander of Joint Forces Headquarters-Department of Defense Information Network a draft plan to implement such zero trust strategy, principles, and model architecture across the networks of their respective components and military departments.

''(2) ELEMENTS.—Each implementation plan transmitted pursuant to paragraph (1) shall include, at a minimum, the following:

''(A) Specific acquisitions, implementations, instrumentations, and operational workflows to be implemented across unclassified and classified networks, operational technology, and weapon systems.

''(B) A detailed schedule with target milestones and required expenditures.

''(C) Interim and final metrics, including a phase migration plan.

''(D) Identification of additional funding, authorities, and policies, as may be required.

''(E) Requested waivers, exceptions to Department of Defense policy, and expected delays.

''(e) IMPLEMENTATION OVERSIGHT.—

''(1) IN GENERAL.—The Chief Information Officer of the Department of Defense shall—

''(A) assess the implementation plans transmitted pursuant to subsection (d)(1) for—

''(i) adequacy and responsiveness to the zero trust strategy, principles, and model architecture required under subsection (a); and

''(ii) appropriate use of enterprise-wide acquisitions;

''(B) ensure, at a high level, the interoperability and compatibility of individual components' Solutions Architectures, including the leveraging of enterprise capabilities where appropriate through standards derivation, policy, and reviews;

''(C) use the annual investment guidance of the Chief to ensure appropriate implementation of such plans, including appropriate use of enterprise-wide acquisitions;

''(D) track use of waivers and exceptions to policy;

''(E) use the Cybersecurity Scorecard to track and drive implementation of Department components; and

''(F) leverage the authorities of the Commander of Joint Forces Headquarters-Department of Defense Information Network and the Director of the Defense Information Systems Agency to begin implementation of such zero trust strategy, principles, and model architecture.

''(2) ASSESSMENTS OF FUNDING.—Not later than March 31, 2024, and annually thereafter, each Principal Cyber Advisor of a military service shall include in the annual budget certification of such military service, as required by section 392a(c)(4) of title 10, United States Code, an assessment of the adequacy of funding requested for each proposed budget for the purposes of carrying out the implementation plan for such military service under subsection (d)(1).

''(f) INITIAL BRIEFINGS.—

''(1) ON MODEL ARCHITECTURE.—Not later than 90 days after finalizing the zero trust strategy, principles, and model architecture required under subsection (a), the Chief Information Officer of the Department of Defense and the Commander of Joint Forces Headquarters-Department of Defense Information Network shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on such zero trust strategy, principles, and model architecture.

''(2) ON IMPLEMENTATION PLANS.—Not later than 90 days after the receipt by the Chief Information Officer of the Department of Defense of an implementation plan transmitted pursuant to subsection (d)(1), the secretary of a military department, in the case of an implementation plan pertaining to a military department or a military service, or the Chief Information Officer of the Department, in the case of an implementation plan pertaining to a remaining component of the Department, as the case may be, shall provide to the congressional defense committees a briefing on such implementation plan.

''(g) ANNUAL BRIEFINGS.—Effective February 1, 2022, at each of the annual cybersecurity budget review briefings of the Chief Information Officer of the Department of Defense and the military services for congressional staff, until January 1, 2030, the Chief Information Officer and the head of each of the military services shall provide updates on the implementation in their respective networks of the zero trust strategy, principles, and model architecture.''

DEMONSTRATION PROGRAM FOR AUTOMATED SECURITY VALIDATION TOOLS

Pub. L. 117–81, div. A, title XV, §1529, Dec. 27, 2021, 135 Stat. 2048, provided that:

''(a) DEMONSTRATION PROGRAM REQUIRED.—Not later than October 1, 2024, the Chief Information Officer of the Department of Defense, acting through the Director of the Defense Information Systems Agency of the Department, shall complete a demonstration program to demonstrate and assess an automated security validation capability to assist the Department by—

''(1) mitigating cyber hygiene challenges;

''(2) supporting ongoing efforts of the Department to assess weapon systems resiliency;

''(3) quantifying enterprise security effectiveness of enterprise security controls, to inform future acquisition decisions of the Department;

''(4) assisting portfolio managers with balancing capability costs and capability coverage of the threat landscape; and

''(5) supporting the Department's Cybersecurity Analysis and Review threat framework.

''(b) CONSIDERATIONS.—In developing capabilities for the demonstration program required under subsection (a), the Chief Information Officer shall consider—

''(1) integration into automated security validation tools of advanced commercially available threat intelligence;

''(2) metrics and scoring of security controls;

''(3) cyber analysis, cyber campaign tracking, and cybersecurity information sharing;

''(4) integration into cybersecurity enclaves and existing cybersecurity controls of security instrumentation and testing capability;

''(5) endpoint sandboxing; and

''(6) use of actual adversary attack methodologies.

''(c) COORDINATION WITH MILITARY SERVICES.—In carrying out the demonstration program required under subsection (a), the Chief Information Officer, acting through the Director of the Defense Information Systems Agency, shall coordinate demonstration program activities with complementary efforts on-going within the military services, defense agencies, and field agencies.

''(d) INDEPENDENT CAPABILITY ASSESSMENT.—In carrying out the demonstration program required under subsection (a), the Chief Information Officer, acting through the Director of the Defense Information Systems Agency and in coordination with the Director, Operational Test and Evaluation, shall perform operational testing to evaluate the operational effectiveness, suitability, and cybersecurity of the capabilities developed under the demonstration program.

''(e) BRIEFING.—

''(1) INITIAL BRIEFING.—Not later than April 1, 2022, the Chief Information Officer shall brief the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on the plans and status of the Chief Information Officer with respect to the demonstration program required under subsection (a).

''(2) FINAL BRIEFING.—Not later than October 31, 2024, the Chief Information Officer shall brief the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on the results and findings of the Chief Information Officer with respect to the demonstration program required under subsection (a).''

CONSIDERATIONS RELATING TO PERMANENTLY BASING UNITED STATES EQUIPMENT OR ADDITIONAL FORCES IN HOST COUNTRIES WITH AT-RISK VENDORS IN 5G OR 6G NETWORKS

Pub. L. 116–283, div. A, title X, §1058, Jan. 1, 2021, 134 Stat. 3856, provided that:

''(a) IN GENERAL.—Prior to basing a major weapon system or additional permanently assigned forces comparable to or larger than a battalion, squadron, or naval combatant in a host country with at-risk 5th generation (in this section referred to as '5G') or sixth generation (in this section referred to as '6G') wireless network equipment, software, or services, including supply chain vulnerabilities identified by the Federal Acquisition Security Council, where United States military personnel and their families will be directly connected or subscribers to networks that include such at-risk equipment, software, and services in their official duties or in the conduct of personal affairs, the Secretary of Defense shall take into consideration the risks to personnel, equipment, and operations of the Department of Defense in the host country posed by current or intended use by such country of 5G or 6G telecommunications architecture provided by at-risk vendors, including Huawei and ZTE, and any steps to mitigate those risks, including—

''(1) any steps being taken by the host country to mitigate any potential risks to the weapon systems, military units, or personnel, and the Department of Defense's assessment of those efforts;

''(2) any steps being taken by the United States Government, separately or in collaboration with the host country, to mitigate any potential risks to the weapon systems, permanently deployed forces, or personnel;

''(3) any defense mutual agreements between the host country and the United States intended to allay the costs of risk mitigation posed by the at-risk infrastructure; and

''(4) any other matters the Secretary determines to be relevant.

''(b) APPLICABILITY.—The requirements under subsection (a)—

''(1) apply with respect to the permanent long-term stationing of equipment and permanently assigned forces; and

''(2) do not apply with respect to the short-term deployment or rotational presence of equipment or forces to a military installation outside the United States in connection with any exercise, dynamic force employment, contingency operation, or combat operation.

''(c) REPORT.—

''(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that contains an assessment of—

''(A) the risk to personnel, equipment, and operations of the Department of Defense in host countries posed by the current or intended use by such countries of 5G or 6G telecommunications architecture provided by at-risk vendors, including Huawei and ZTE; and

''(B) measures required to mitigate the risk described in paragraph (1).

''(2) FORM.—The report required by paragraph (1) shall be submitted in a classified form with an unclassified summary.

''(d) MAJOR WEAPON SYSTEM DEFINED.—In this section, the term 'major weapon system' has the meaning given that term in section 2379(f) of title 10, United States Code [now 10 U.S.C. 3455(f)].''

RESPONSIBILITY FOR CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION OF THE DEFENSE INDUSTRIAL BASE

Pub. L. 116–283, div. A, title XVII, §1724, Jan. 1, 2021, 134 Stat. 4111, as amended by Pub. L. 118–31, div. A, title XV, §1511, Dec. 22, 2023, 137 Stat. 541, provided that:

''(a) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term 'critical infrastructure' has the meaning given such term in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)).

''(b) DESIGNATION.—Not later than 30 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2024 [Dec. 22, 2023], the Secretary of Defense shall designate a principal staff assistant from within the Office of the Secretary of Defense who shall serve as the coordinating authority for cybersecurity issues relating to the defense industrial base.

''(c) RESPONSIBILITIES.—As the coordinating authority for cybersecurity issues relating to the defense industrial base, the principal staff assistant designated under subsection (b) shall synchronize, harmonize, deconflict, and coordinate all policies and programs germane to defense industrial base cybersecurity, including the following:

''(1) The Sector Risk Management Agency functions under Presidential Policy Directive-21 the Department of Defense has assigned to the Under Secretary of Defense for Policy for implementation.

''(2) The Under Secretary of Defense for Acquisition and Sustainment's policies and programs germane to contracting and contractual enforcement as such relate to cybersecurity assessment and assistance, and industrial base health and security.

''(3) The Under Secretary of Defense for Intelligence and Security's policies and programs germane to physical security, information security, industrial security, acquisition security and cybersecurity, all source intelligence, classified threat intelligence sharing related to defense industrial base cybersecurity activities, counterintelligence, and foreign ownership control or influence, including the Defense Intelligence Agency and National Security Agency support provided to the Department of Defense – Defense Industrial Base Collaborative Information Sharing Environment and cyber intrusion damage assessment analysis as part of defense industrial base cybersecurity activities.

''(4) The Department of Defense Chief Information Officer's policies and programs for cybersecurity standards and integrating cybersecurity threat intelligence-sharing activities and enhancing Department of Defense and defense industrial base cyber situational awareness.

''(5) The Under Secretary of Defense for Research and Engineering's policies and programs germane to protection planning requirements of emerging technologies as such relate to cybersecurity assessment and assistance, and industrial base health and security.

''(6) Other Department of Defense components' policies and programs germane to the cybersecurity of the defense industrial base, including the policies and programs of the military services and the combatant commands.

''(d) ADDITIONAL FUNCTIONS.—In carrying out this section, the principal staff assistant designated under subsection (b) shall—

''(1) coordinate or facilitate coordination with relevant Federal departments and agencies, defense industrial base entities, independent regulatory agencies, and with State, local, territorial, and Tribal entities, as appropriate;

''(2) facilitate or coordinate the provision of incident management support to defense industrial base entities, as appropriate;

''(3) facilitate or coordinate the provision of technical assistance to and consultations with defense industrial base entities to identify cyber or cyber-physical vulnerabilities and minimize the damage of potential incidents, as appropriate; and

''(4) support or facilitate the supporting of the statutorily required reporting requirements of such relevant Federal departments and agencies by providing or facilitating the provision to such departments and agencies on an annual basis relevant critical infrastructure information, as appropriate.

''(e) DEPARTMENT OF DEFENSE ROLES AND RESPONSIBILITIES.—No later than 180 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2024 [Dec. 22, 2023], the Secretary of Defense shall brief the Committees on Armed Services of the Senate and the House of Representatives on the following issues:

''(1) A plan for implementation of this section, including an assessment of the roles and responsibilities of entities across the Department of Defense and mechanisms and processes for coordination of policy and programs germane to defense industrial base cybersecurity.

''(2) An analysis of the feasibility and advisability of separating cybersecurity functions of a Sector Risk Management Agency pursuant to section 9002 of the National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) from non-cybersecurity functions of a Sector Risk Management Agency.''

IMPROVING THE TRAINING WITH INDUSTRY PROGRAM

Pub. L. 116–283, div. A, title XVII, §1726(b), Jan. 1, 2021, 134 Stat. 4116, provided that:

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Jan. 1, 2021], the Principal Cyber Advisor of the Department of Defense, in consultation with the Principal Cyber Advisors of the military services and the Under Secretary of Defense for Personnel and Readiness, shall submit to the Secretary of Defense and the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a review of the current utilization and utility of the Training With Industry (TWI) programs, including relating to the following:

''(A) Recommendations regarding how to improve and better utilize such programs, including regarding individuals who have completed such programs.

''(B) An implementation plan to carry out such recommendations.

''(2) ADDITIONAL.—Not later than 90 days after the submission of the report required under paragraph (1), the Secretary of Defense shall carry out such elements of the implementation plan required under paragraph (1)(B) as the Secretary considers appropriate and notify the congressional defense committees of the determinations of the Secretary relating thereto.''

REPORTING REQUIREMENTS FOR CROSS DOMAIN INCIDENTS AND EXEMPTIONS TO POLICIES FOR INFORMATION TECHNOLOGY

Pub. L. 116–283, div. A, title XVII, §1727, Jan. 1, 2021, 134 Stat. 4117, as amended by Pub. L. 118–159, div. A, title XV, §1511, Dec. 23, 2024, 138 Stat. 2136, provided that:

''(a) INCIDENT REPORTING.—

''(1) IN GENERAL.—Effective beginning on the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense and the secretaries of the military services shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a monthly report in writing that documents each instance or indication of a cross-domain incident within the Department of Defense.

''(2) PROCEDURES.—The Secretary of Defense shall submit to the congressional defense committees procedures for complying with the requirements of paragraph (1) consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify such committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

''(3) DEFINITION.—In this subsection, the term 'cross domain incident' means any unauthorized connection of any duration between software, hardware, or both that is either used on, or designed for use on a network or system built for classified data, and systems not accredited or authorized at the same or higher classification level, including systems on the public internet, regardless of whether the unauthorized connection is later determined to have resulted in the exfiltration, exposure, or spillage of data across the cross domain connection.

''(b) EXEMPTIONS TO POLICY FOR INFORMATION TECHNOLOGY.—Not later than six months after the date of the enactment of this Act and biannually thereafter, the Secretary of Defense and the secretaries of the military services shall submit to the congressional defense committees a report in writing that enumerates and details each current exemption to information technology policy, interim Authority To Operate (ATO) order, or both. Each such report shall include other relevant information pertaining to each such exemption, including relating to the following:

''(1) Risk categorization.

''(2) Duration.

''(3) Estimated time remaining.

''(c) TERMINATION DATE.—The requirement of the Secretary of Defense to submit a monthly report under subsection (a) shall terminate on December 31, 2025.''

PILOT PROGRAM ON CYBERSECURITY CAPABILITY METRICS

Pub. L. 116–283, div. A, title XVII, §1733, Jan. 1, 2021, 134 Stat. 4123, provided that:

''(a) PILOT PROGRAM REQUIRED.—The Secretary of Defense, acting through the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command, shall conduct a pilot program to assess the feasibility and advisability of developing and using speed-based metrics to measure the performance and effectiveness of security operations centers and cyber security service providers in the Department of Defense.

''(b) REQUIREMENTS.—

''(1) DEVELOPMENT OF METRICS.—(A) Not later than July 1, 2021, the Chief Information Officer and the Commander shall jointly develop metrics described in subsection (a) to carry out the pilot program under such subsection.

''(B) The Chief Information Officer and the Commander shall ensure that the metrics developed under subparagraph (A) are commensurate with the representative timelines of nation-state and non-nation-state actors when gaining access to, and compromising, Department networks.

''(2) USE OF METRICS.—(A) Not later than December 1, 2021, the Secretary shall, in carrying out the pilot program required by subsection (a), begin using the metrics developed under paragraph (1) of this subsection to assess select security operations centers and cyber security service providers, which the Secretary shall select specifically for purposes of the pilot program, for a period of not less than four months.

''(B) In carrying out the pilot program under subsection (a), the Secretary shall evaluate the effectiveness of operators, capabilities available to operators, and operators' tactics, techniques, and procedures.

''(c) AUTHORITIES.—In carrying out the pilot program under subsection (a), the Secretary may—

''(1) assess select security operations centers and cyber security service providers—

''(A) over the course of their mission performance; or

''(B) in the testing and accreditation of cybersecurity products and services on test networks designated pursuant to section 1658 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) [set out as a note below]; and

''(2) assess select elements' use of security orchestration and response technologies, modern endpoint security technologies, Big Data Platform instantiations, and technologies relevant to zero trust architectures.

''(d) BRIEFING.—

''(1) IN GENERAL.—Not later than March 1, 2022, the Secretary shall brief the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on the findings of the Secretary with respect to the pilot program required by subsection (a).

''(2) ELEMENTS.—The briefing provided under paragraph (1) shall include the following:

''(A) The pilot metrics developed under subsection (b)(1).

''(B) The findings of the Secretary with respect to the assessments carried out under subsection (b)(2).

''(C) An analysis of the utility of speed-based metrics in assessing security operations centers and cyber security service providers.

''(D) An analysis of the utility of the extension of the pilot metrics to or speed-based assessment of the Cyber Mission Forces.

''(E) An assessment of the technical and procedural measures that would be necessary to meet the speed-based metrics developed and applied in the pilot program.''

INTEGRATION OF DEPARTMENT OF DEFENSE USER ACTIVITY MONITORING AND CYBERSECURITY

Pub. L. 116–283, div. A, title XVII, §1735, Jan. 1, 2021, 134 Stat. 4125, provided that:

''(a) INTEGRATION OF PLANS, CAPABILITIES, AND SYSTEMS.—The Secretary of Defense shall integrate the plans, capabilities, and systems for user activity monitoring, and the plans, capabilities, and systems for endpoint cybersecurity and the collection of metadata on network activity for cybersecurity to enable mutual support and information sharing.

''(b) REQUIREMENTS.—In carrying out subsection (a), the Secretary shall—

''(1) consider using the Big Data Platform instances that host cybersecurity metadata for storage and analysis of all user activity monitoring data collected across the Department of Defense Information Network at all security classification levels;

''(2) develop policies and procedures governing access to user activity monitoring data or data derived from user activity monitoring by cybersecurity operators; and

''(3) develop processes and capabilities for using metadata on host and network activity for user activity monitoring in support of the insider threat mission.

''(c) CONGRESSIONAL BRIEFING.—Not later than October 1, 2021, the Secretary shall provide a briefing to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] on actions taken to carry out this section.''

ASSESSMENT ON DEFENSE INDUSTRIAL BASE PARTICIPATION IN A THREAT INFORMATION SHARING PROGRAM

Pub. L. 116–283, div. A, title XVII, §1737, Jan. 1, 2021, 134 Stat. 4127, provided that:

''(a) DEFENSE INDUSTRIAL BASE THREAT INFORMATION PROGRAM ASSESSMENT.—Not later than 270 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall complete an assessment of the feasibility, suitability, and definition of, and resourcing required to establish, a defense industrial base threat information sharing program to collaborate and share threat information with, and obtain threat information from, the defense industrial base.

''(b) ELEMENTS.—The assessment regarding the establishment of a defense industrial base threat information sharing program under subsection (a) shall include evaluation of the following:

''(1) The feasibility and suitability of, and requirements for, the establishment of a defense industrial base threat information sharing program, including cybersecurity incident reporting requirements applicable to the defense industrial base that—

''(A) extend beyond mandatory cybersecurity incident reporting requirements as in effect on the day before the date of the enactment of this Act;

''(B) set specific, consistent timeframes for all categories of cybersecurity incident reporting;

''(C) establish a single clearinghouse for all mandatory cybersecurity incident reporting to the Department of Defense, including incidents involving covered unclassified information, and classified information; and

''(D) provide that, unless authorized or required by another provision of law or the element of the defense industrial base making the report consents, nonpublic information of which the Department becomes aware only because of a report provided pursuant to the program shall be disseminated and used only for a cybersecurity purpose (as such term is defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)) and in support of national defense activities.

''(2) A mechanism for developing a shared and real-time picture of the threat environment.

''(3) Options for joint, collaborative, and co-located analytics.

''(4) Possible investments in technology and capabilities to support automated detection and analysis across the defense industrial base.

''(5) Coordinated information tipping, sharing, and deconfliction, as necessary, with relevant Federal Government agencies with similar information sharing programs.

''(6) Processes for direct sharing of threat information related to a specific defense industrial base entity with such entity.

''(7) Mechanisms for providing defense industrial base entities with clearances for national security information access, as appropriate.

''(8) Requirements to consent to queries of foreign intelligence collection databases related to a specific defense industrial base entity as a condition of participation in the threat information sharing program.

''(9) Recommendations with respect to threat information sharing program participation, including the following:

''(A) Incentives for defense industrial base entities to participate in the threat information sharing program.

''(B) Mandating minimum levels of threat information sharing program participation for any entity that is part of the defense industrial base.

''(C) Procurement prohibitions on any defense industrial base entity that are not in compliance with the requirements of the threat information sharing program.

''(D) Waiver authority and criteria.

''(E) Adopting tiers of requirements for participation within the threat information sharing program based on—

''(i) the role of and relative threats related to defense industrial base entities; and

''(ii) Cybersecurity Maturity Model Certification level.

''(10) Options to utilize an existing federally recognized information sharing program to satisfy the re-

quirement for a threat information sharing program if—

''(A) the existing program includes, or is modified to include, two-way sharing of threat information that is specifically relevant to the defense industrial base; and

''(B) such a program is coordinated with other Federal Government agencies with existing information sharing programs where overlap occurs.

''(11) Methods to encourage participation of defense industrial base entities in appropriate private sector information sharing and analysis centers (ISACs).

''(12) Methods to coordinate collectively with defense industrial base entities to consider methods for mitigating compliance costs.

''(13) The resources needed, governance roles and structures required, and changes in regulation or law needed for execution of a threat information sharing program, as well as any other considerations determined relevant by the Secretary.

''(14) Identification of any barriers that would prevent the establishment of a defense industrial base threat information sharing program.

''(c) CONSULTATION.—In conducting the assessment required under subsection (a), the Secretary of Defense shall consult with and solicit recommendations from representative industry stakeholders across the defense industrial base regarding the elements described in subsection (b) and potential stakeholder costs of compliance.

''(d) DETERMINATION AND BRIEFING.—Upon completion of the assessment required under subsection (a), the Secretary of Defense shall make a determination regarding the establishment by the end of fiscal year 2021 of a defense industrial base threat information sharing program and provide a briefing to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on—

''(1) the findings of the Secretary with respect to such assessment and such determination; and

''(2) such implementation plans as the Secretary may have arising from such findings.

''(e) IMPLEMENTATION.—If the Secretary of Defense makes a positive determination pursuant to subsection (d) of the feasibility and suitability of establishing a defense industrial base threat information sharing program, the Secretary shall establish such program. Not later than 180 days after a positive determination, the Secretary of Defense shall promulgate such rules and regulations as are necessary to establish the defense industrial base threat information sharing program under this section.''

ASSISTANCE FOR SMALL MANUFACTURERS IN THE DEFENSE INDUSTRIAL SUPPLY CHAIN ON MATTERS RELATING TO CYBERSECURITY

Pub. L. 116–283, div. A, title XVII, §1738, Jan. 1, 2021, 134 Stat. 4129, provided that:

''(a) IN GENERAL.—Subject to the availability of appropriations, the Secretary of Defense, in consultation with the Director of the National Institute of Standards and Technology, may award financial assistance to a Center for the purpose of providing cybersecurity services to small manufacturers.

''(b) CRITERIA.—If the Secretary carries out subsection (a), the Secretary, in consultation with the Director, shall establish and publish on the grants.gov website, or successor website, criteria for selecting recipients for financial assistance under this section.

''(c) USE OF FINANCIAL ASSISTANCE.—Financial assistance under this section—

''(1) shall be used by a Center to provide small manufacturers with cybersecurity services, including—

''(A) compliance with the cybersecurity requirements of the Department of Defense Supplement to the Federal Acquisition Regulation, including awareness, assessment, evaluation, preparation, and implementation of cybersecurity services; and

''(B) achieving compliance with the Cybersecurity Maturity Model Certification framework of the Department of Defense; and

''(2) may be used by a Center to employ trained personnel to deliver cybersecurity services to small manufacturers.

''(d) BIENNIAL REPORTS.—

''(1) IN GENERAL.—Not less frequently than once every two years, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Science, Space, and Technology of the House of Representatives a report on financial assistance awarded under this section.

''(2) CONTENTS.—To the extent practicable, each report submitted under paragraph (1) shall include the following with respect to the years covered by each such report:

''(A) The number of small manufacturers assisted.

''(B) A description of the cybersecurity services provided.

''(C) A description of the cybersecurity matters addressed.

''(D) An analysis of the operational effectiveness and cost-effectiveness of such cybersecurity services.

''(e) TERMINATION.—The authority of the Secretary to award financial assistance under this section shall terminate on the date that is five years after the date of the enactment of this section [Jan. 1, 2021].

''(f) DEFINITIONS.—In this section:

''(1) CENTER.—The term 'Center' has the meaning given such term in section 25(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278k(a)).

''(2) SMALL MANUFACTURER.—The term 'small manufacturer' has the meaning given such term in section 1644(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2224 note).''

ASSESSMENT ON DEFENSE INDUSTRIAL BASE CYBERSECURITY THREAT HUNTING PROGRAM

Pub. L. 116–283, div. A, title XVII, §1739, Jan. 1, 2021, 134 Stat. 4130, provided that:

''(a) ASSESSMENT REQUIRED.—Not later than 270 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall complete an assessment of the feasibility, suitability, definition of, and resourcing required to establish a defense industrial base cybersecurity threat hunting program to actively identify cybersecurity threats and vulnerabilities within the defense industrial base.

''(b) ELEMENTS.—The assessment required under section [sic] (a) shall include evaluation of the following:

''(1) Existing defense industrial base cybersecurity threat hunting policies and programs, including the threat hunting elements at each level of the compliance-based Cybersecurity Maturity Model Certification program of the Department of Defense, including requirements germane to continuous monitoring, discovery, and investigation of anomalous activity indicative of a cybersecurity incident.

''(2) The suitability of a continuous cybersecurity threat hunting program, as a supplement to the cyber hygiene requirements of the Cybersecurity Maturity Model Certification, including consideration of the following:

''(A) Collection and analysis of metadata on network activity to detect possible intrusions.

''(B) Rapid investigation and remediation of possible intrusions.

''(C) Requirements for mitigating any vulnerabilities identified pursuant to the cybersecurity threat hunting program.

''(D) Mechanisms for the Department of Defense to share with entities in the defense industrial base malicious code, indicators of compromise, and insights on the evolving threat landscape.

''(3) Recommendations with respect to cybersecurity threat hunting program participation

of prime contractors and subcontractors, including relating to the following:

''(A) Incentives for defense industrial base entities to share with the Department of Defense threat and vulnerability information collected pursuant to threat monitoring and hunting activities.

''(B) Mandating minimum levels of program participation for any defense industrial base entity.

''(C) Procurement prohibitions on any defense industrial base entity that is not in compliance with the requirements of the cybersecurity threat hunting program.

''(D) Waiver authority and criteria.

''(E) Consideration of a tiered cybersecurity threat hunting program that takes into account the following:

''(i) The cybersecurity maturity of defense industrial base entities.

''(ii) The roles of such entities.

''(iii) Whether each such entity possesses classified information or controlled unclassified information and covered defense networks.

''(iv) The covered defense information to which each such entity has access as a result of contracts with the Department of Defense.

''(4) Whether the continuous cybersecurity threat-hunting program described in paragraph (2) should be conducted by—

''(A) qualified prime contractors or subcontractors;

''(B) accredited third-party cybersecurity vendors;

''(C) with contractor consent—

''(i) United States Cyber Command; or

''(ii) a component of the Department of Defense other than United States Cyber Command;

''(D) the deployment of network sensing technologies capable of identifying and filtering malicious network traffic; or

''(E) a combination of the entities specified in subparagraphs (A) through (D).

''(5) The resources necessary, governance structures or changes in regulation or law needed, and responsibility for execution of a defense industrial base cybersecurity threat hunting program, as well as any other considerations determined relevant by the Secretary.

''(6) A timelime [sic] for establishing the defense industrial base cybersecurity threat hunting program not later than two years after the date of the enactment of this Act [Jan. 1, 2021].

''(7) Identification of any barriers that would prevent such establishment.

''(c) CONSULTATION.—In conducting the assessment required under subsection (a), the Secretary of Defense shall consult with and solicit recommendations from representative industry stakeholders across the defense industrial base regarding the elements described in subsection (b) and potential stakeholder costs of compliance.

''(d) DETERMINATION AND BRIEFING.—Upon completion of the assessment required under subsection (a), the Secretary of Defense shall make a determination regarding the establishment of a defense industrial base cybersecurity threat hunting program and provide a briefing to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives on—

''(1) the findings of the Secretary with respect to such assessment and such determination; and

''(2) such implementation plans as the Secretary may have arising from such findings.

''(e) IMPLEMENTATION.—If the Secretary of Defense makes a positive determination pursuant to subsection (d) of the feasibility and suitability of establishing a defense industrial base threat cybersecurity threat hunting program, the Secretary shall establish such program. Not later than 180 days after a positive determination, the Secretary of Defense shall promulgate such rules and regulations as are necessary to establish the defense industrial base cybersecurity threat hunting program under this section.''

ROLE OF CHIEF INFORMATION OFFICER IN IMPROVING ENTERPRISE-WIDE CYBERSECURITY

Pub. L. 116–92, div. A, title XVI, §1641, Dec. 20, 2019, 133 Stat. 1750, provided that:

''(a) IN GENERAL.—In carrying out the responsibilities established in section 142 of title 10, United States Code, the Chief Information Officer of the Department of Defense shall, to the maximum extent practicable, ensure that the cybersecurity programs and capabilities of the Department—

''(1) fit into an enterprise-wide cybersecurity architecture;

''(2) are maximally interoperable with each other, including those programs and capabilities deployed by the components of the Department;

''(3) enhance enterprise-level visibility and responsiveness to threats; and

''(4) are developed, procured, instituted, and managed in a cost-efficient manner, exploiting economies of scale and enterprise-wide services and discouraging unnecessary customization and piecemeal acquisition.

''(b) REQUIREMENTS.—In carrying out subsection (a), the Chief Information Officer shall—

''(1) manage and modernize the cybersecurity architecture of the Department, including—

''(A) ensuring the cybersecurity architecture of the Department maximizes cybersecurity capability, network, and endpoint activity data sharing across Department components;

''(B) ensuring the cybersecurity architecture of the Department supports improved automaticity of cybersecurity detection and response; and

''(C) modernizing and configuring the Department's standardized deployed perimeter, network-level, and endpoint capabilities to improve interoperability, meet pressing capability needs, and negate common adversary tactics, techniques, and procedures;

''(2) establish mechanisms to enable and mandate, as necessary, cybersecurity capability and network and endpoint activity data-sharing across Department components;

''(3) make mission data, through data tagging, automatic transmission, and other means, accessible and discoverable by Department components other than owners of such mission data;

''(4) incorporate into the cybersecurity architecture of the Department emerging cybersecurity technologies from the Defense Advanced Research Projects Agency, the Strategic Capabilities Office, the Defense Innovation Unit, the laboratories of the military departments, and the commercial sector;

''(5) ensure that the Department possesses the necessary computing infrastructure, through technology refresh, installation or acquisition of bandwidth, and the use of cloud computing power, to host and enable necessary cybersecurity capabilities; and

''(6) utilize the Department's cybersecurity expertise to improve cybersecurity performance, operations, and acquisition, including—

''(A) the cybersecurity testing, architecting, and engineering expertise of the National Security Agency; and

''(B) the technology policy, workforce, and engineering expertise of the Defense Digital Service.''

CONTROL AND ANALYSIS OF DEPARTMENT OF DEFENSE DATA STOLEN THROUGH CYBERSPACE

Pub. L. 116–92, div. A, title XVI, §1646, Dec. 20, 2019, 133 Stat. 1753, provided that:

''(a) REQUIREMENTS.—If the Secretary of Defense determines that significant Department of Defense data may have been stolen through cyberspace and evidence of theft of the data in question—

''(1) is in the possession of a component of the Department, the Secretary shall—

''(A) either transfer or replicate and transfer such Department data in a prompt and secure manner to a secure repository with access by Department personnel appropriately limited on a need-to-know basis or otherwise ensure such consistent access to the relevant data by other means;

''(B) ensure the Department applies such automated analytic tools and capabilities to the repository of potentially compromised data as are necessary to rapidly understand the scope and effect of the potential compromise;

''(C) for high priority and mission critical Department systems, develop analytic products that characterize the scope of data compromised;

''(D) ensure that relevant mission-affected entities in the Department are made aware of the theft or possible theft and, as damage assessment and mitigation proceeds, are kept apprised of the extent of the data stolen; and

''(E) ensure that Department counterintelligence organizations are—

''(i) fully integrated with any damage assessment team assigned to the breach;

''(ii) fully informed of the data that have or potentially have been stolen and the effect of such theft; and

''(iii) provided resources and tasked, in conjunction with subject matter experts and responsible authorities, to immediately and appropriately respond, including through the development and execution of relevant countermeasures, to any breach involving espionage and data theft; or

''(2) is in the possession of or under controls or restrictions imposed by the Federal Bureau of Investigation, or a national counterintelligence or intelligence organization, the Secretary shall determine, jointly with the Director of the Federal Bureau of Investigation or the Director of National Intelligence, as appropriate, the most expeditious process, means, and conditions for carrying out the activities otherwise required by paragraph (1).

''(b) RECOMMENDATIONS.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] such recommendations as the Secretary may have for legislative or administrative action to address such barriers that may be inhibiting the implementation of this section.''

USE OF NATIONAL SECURITY AGENCY CYBERSECURITY EXPERTISE TO SUPPORT EVALUATION OF COMMERCIAL CYBERSECURITY PRODUCTS

Pub. L. 116–92, div. A, title XVI, §1647, Dec. 20, 2019, 133 Stat. 1754, as amended by Pub. L. 116–283, div. A, title X, §1081(c)(7), Jan. 1, 2021, 134 Stat. 3873, provided that:

''(a) ADVISORY MISSION.—The National Security Agency shall, as a mission in its role in securing the information systems of the Department of Defense, advise and assist the Department of Defense in its evaluation and adoption of cybersecurity products and services from industry, especially the commercial cybersecurity sector.

''(b) PROGRAM TO IMPROVE ACQUISITION OF CYBERSECURITY PRODUCTS AND SERVICES.—

''(1) ESTABLISHMENT.—Consistent with subsection (a), the Director of the National Security Agency shall establish a permanent program consisting of market research, testing, and expertise transmission, or augments to existing programs, to improve the evaluation by the Department of Defense of cybersecurity products and services.

''(2) REQUIREMENTS.—Under the program established pursuant to paragraph (1), the Director shall, independently and at the request of the components of the Department of Defense—

''(A) test and evaluate commercially available cybersecurity products and services using—

''(i) generally known cyber operations techniques; and

''(ii) tools and cyber operations techniques and advanced tools and techniques available to the National Security Agency;

''(B) develop and establish standard procedures, techniques, and threat-informed metrics to perform the testing and evaluation required by subparagraph (A); and

''(C) advise the Chief Information Officer and the components of the Department of Defense on the merits and disadvantages of evaluated cybersecurity products, including with respect to—

''(i) any synergies between products;

''(ii) value;

''(iii) matters relating to operation and maintenance; and

''(iv) matters relating to customization requirements.

''(3) LIMITATIONS.—The program established under paragraph (1) may not—

''(A) be used to accredit cybersecurity products and services for use by the Department;

''(B) create approved products lists; or

''(C) be used for the procurement and fielding of cybersecurity products on behalf of the Department.''

[Pub. L. 116–283, div. A, title X, §1081(c), Jan. 1, 2021, 134 Stat. 3873, provided that the amendment made by section 1081(c)(7) of Pub. L. 116–283 to section 1647 of Pub. L. 116–92, set out above, is effective as of Dec. 20, 2020 (probably should be Dec. 20, 2019) and as if included in Pub. L. 116–92.]

FRAMEWORK TO ENHANCE CYBERSECURITY OF THE UNITED STATES DEFENSE INDUSTRIAL BASE

Pub. L. 116–92, div. A, title XVI, §1648, Dec. 20, 2019, 133 Stat. 1755, as amended by Pub. L. 117–81, div. A, title XV, §1526, Dec. 27, 2021, 135 Stat. 2043, provided that:

''(a) FRAMEWORK REQUIRED.—Not later than 180 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2022 [Dec. 27, 2021], the Secretary of Defense shall develop a consistent, comprehensive framework to enhance cybersecurity for the United States defense industrial base.

''(b) ELEMENTS.—The framework developed pursuant to subsection (a) shall include the following:

''(1) Identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors.

''(2) Roles and responsibilities of the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Intelligence and Security, the Chief Information Officer, the Director of the Protecting Critical Technologies Task Force, and the Secretaries of the military departments relating to the following:

''(A) Establishing and ensuring compliance with cybersecurity standards, regulations, and policies.

''(B) Deconflicting existing cybersecurity standards, regulations, and policies.

''(C) Coordinating with and providing assistance to the defense industrial base for cybersecurity matters, particularly as relates to the programs and processes described in paragraphs (8) and (9).

''(D) Management and oversight of the acquisition process, including responsibility determination, solicitation, award, and contractor management, relating to cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements.

''(3) The responsibilities of the prime contractors, and all subcontractors in the supply chain, for implementing the required cybersecurity standards, regulations, metrics, ratings, third-party certifications, and requirements identified under paragraph (1).

''(4) Definitions for 'Controlled Unclassified Information' (CUI) and 'For Official Use Only' (FOUO),

policies regarding protecting information designated as either of such, and an explanation of the 'DoD CUI Program' and Department of Defense compliance with the responsibilities specified in Department of Defense Instruction (DoDI) 5200.48, 'Controlled Unclassified Information (CUI),' including the following:

''(A) The extent to which the Department of Defense is identifying whether information is CUI via a contracting vehicle and marking documents, material, and media containing such information in a clear and consistent manner.

''(B) Recommended regulatory or policy changes to ensure consistency and clarity in CUI identification and marking requirements.

''(C) Circumstances under which commercial information is considered CUI, and any impacts to the commercial supply chain associated with security and marking requirements pursuant to this paragraph.

''(D) Benefits and drawbacks of requiring all CUI to be marked with a unique CUI legend, versus requiring that all data marked with an appropriate restricted legend be handled as CUI.

''(E) The extent to which the Department of Defense clearly delineates Federal Contract Information (FCI) from CUI.

''(F) Examples or scenarios to illustrate information that is and is not CUI.

''(5) Methods and programs for managing controlled unclassified information, and for limiting the presence of unnecessary sensitive information on contractor networks.

''(6) A plan to provide implementation guidance, education, manuals, and, as necessary, direct technical support or assistance, to contractors on matters relating to cybersecurity.

''(7) Quantitative metrics for assessing the effectiveness of the overall framework over time, with respect to the exfiltration of controlled unclassified information from the defense industrial base.

''(8) A comprehensive list of current and planned Department of Defense programs to assist the defense industrial base with cybersecurity compliance requirements of the Department, including those programs that provide training, expertise, and funding, and maintain approved security products lists and approved providers lists.

''(9) Processes for enhanced threat information sharing between the Department of Defense and the defense industrial base.

''(c) MATTERS FOR CONSIDERATION.—In developing the framework pursuant to subsection (a), the Secretary shall consider the following:

''(1) Designating an official to be responsible for the cybersecurity of the defense industrial base.

''(2) Risk-based methodologies, standards, metrics, and tiered cybersecurity requirements for the defense industrial base, including third-party certifications such as the Cybersecurity Maturity Model Certification pilot program, as the basis for a mandatory Department standard.

''(3) Tailoring cybersecurity requirements for small- and medium-sized contractors based on a risk-based approach.

''(4) Ensuring a consistent approach across the Department to cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements of the defense industrial base.

''(5) Ensuring the Department's traceability and visibility of cybersecurity compliance of suppliers to all levels of the supply chain.

''(6) Evaluating incentives and penalties for cybersecurity performance of suppliers.

''(7) Integrating cybersecurity and traditional counterintelligence measures, requirements, and programs.

''(8) Establishing a secure software development environment (DevSecOps) in a cloud environment inside the perimeter of the Department for contractors to perform their development work.

''(9) Establishing a secure cloud environment through which contractors may access the data of the Department needed for their contract work.

''(10) An evaluation of the resources and utilization of Department programs to assist the defense industrial base in complying with cybersecurity compliance requirements referred to in subsection (b)(1).

''(11) Technological means, operational concepts, reference architectures, offensive counterintelligence operation concepts, and plans for operationalization to complicate adversary espionage, including honeypotting and data obfuscation.

''(12) Implementing enhanced security vulnerability assessments for contractors working on critical acquisition programs, technologies, manufacturing capabilities, and research areas.

''(13) Identifying ways to better leverage technology and employ machine learning or artificial intelligence capabilities, such as Internet Protocol monitoring and data integrity capabilities, to be applied to contractor information systems that host, receive, or transmit controlled unclassified information.

''(14) Developing tools to easily segregate program data to only allow subcontractors access to their specific information.

''(15) Appropriate communications of threat assessments of the defense industrial base to the acquisition workforce at all classification levels.

''(16) A single Sector Coordinating Council for the defense industrial base.

''(17) Appropriate communications with the defense industrial base on the impact of cybersecurity requirements in contracting and procurement decisions.

''(d) CONSULTATION.—In developing the framework required pursuant to subsection (a), the Secretary shall consult with the following:

''(1) Industry groups representing the defense industrial base.

''(2) Contractors in the defense industrial base.

''(3) The Director of the National Institute of Standards and Technology.

''(4) The Secretary of Energy.

''(5) The Director of National Intelligence.

''(6) Relevant Federal regulatory agencies.

''(e) BRIEFING.—

''(1) IN GENERAL.—Not later than March 11, 2020, the Secretary of Defense shall provide the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] with a briefing on the framework developed pursuant to subsection (a).

''(2) CONTENTS.—The briefing required by paragraph (1) shall include the following:

''(A) An overview of the framework developed pursuant to subsection (a).

''(B) Identification of such pilot programs as the Secretary considers may be required to improve the cybersecurity of the defense industrial base.

''(C) Implementation timelines and identification of costs.

''(D) Such recommendations as the Secretary may have for legislative action to improve the cybersecurity of the defense industrial base.

''(f) QUARTERLY BRIEFINGS.—

''(1) IN GENERAL.—Not less frequently than once each quarter after the briefing provided pursuant to subsection (e) until February 1, 2022, the Secretary of Defense shall brief the congressional defense committees on the status of development and implementation of the framework developed pursuant to subsection (a).

''(2) COORDINATION WITH OTHER BRIEFINGS.—Each briefing under paragraph (1) shall be conducted in conjunction with a quarterly briefing under section 484(a) of title 10, United States Code.

''(3) ELEMENTS.—Each briefing under paragraph (1) shall include the following:

''(A) The current status of the development and implementation of the framework developed pursuant to subsection (a).

''(B) A description of the efforts undertaken by the Secretary to evaluate the matters for consideration set forth in subsection (c).

''(C) The current status of any pilot programs the Secretary is carrying out to develop the framework.''

DESIGNATION OF TEST NETWORKS FOR TESTING AND ACCREDITATION OF CYBERSECURITY PRODUCTS AND SERVICES

Pub. L. 116–92, div. A, title XVI, §1658, Dec. 20, 2019, 133 Stat. 1769, provided that:

''(a) DESIGNATION.—Not later than April 1, 2020, the Secretary of Defense shall designate, for use by the Defense Information Systems Agency and such other components of the Department of Defense as the Secretary considers appropriate, three test networks for the testing and accreditation of cybersecurity products and services.

''(b) REQUIREMENTS.—The networks designated under subsection (a) shall—

''(1) be of sufficient scale to realistically test cybersecurity products and services;

''(2) feature substantially different architectures and configurations;

''(3) be live, operational networks; and

''(4) feature cybersecurity processes, tools, and technologies that are appropriate for test purposes and representative of the processes, tools, and technologies that are widely used throughout the Department.

''(c) ACCESS.—Upon request, information generated in the testing and accreditation of cybersecurity products and services shall be made available to the Office of the Director, Operational Test and Evaluation.''

PROCEDURES AND REPORTING REQUIREMENT ON CYBERSECURITY BREACHES AND LOSS OF PERSONALLY IDENTIFIABLE INFORMATION AND CONTROLLED UNCLASSIFIED INFORMATION

Pub. L. 115–232, div. A, title XVI, §1639, Aug. 13, 2018, 132 Stat. 2129, provided that:

''(a) IN GENERAL.—In the event of a significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces, or a significant loss of controlled unclassified information by a cleared defense contractor, the Secretary of Defense shall promptly submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] notice in writing of such loss. Such notice may be submitted in classified or unclassified formats.

''(b) PROCEDURES.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirement of subsection (a). Such procedures shall be consistent with the national security of the United States, the protection of operational integrity, the protection of personally identifiable information of civilian and uniformed members of the Armed Forces, and the protection of controlled unclassified information.

''(c) DEFINITIONS.—In this section:

''(1) SIGNIFICANT LOSS OF CONTROLLED UNCLASSIFIED INFORMATION.—The term 'significant loss of controlled unclassified information' means an intentional, accidental, or otherwise known theft, loss, or disclosure of Department of Defense programmatic or technical controlled unclassified information the loss of which would have significant impact or consequence to a program or mission of the Department of Defense, or the loss of which is of substantial volume.

''(2) SIGNIFICANT LOSS OF PERSONALLY IDENTIFIABLE INFORMATION.—The term 'significant loss of personally identifiable information' means an intentional, accidental, or otherwise known disclosure of information that can be used to distinguish or trace an individual's identity, such as the name, Social Security number, date and place of birth, biometric records, home or other phone numbers, or other demographic, personnel, medical, or financial information, involving 250 or more civilian or uniformed members of the Armed Forces.''

MATTERS PERTAINING TO THE SHARKSEER CYBERSECURITY PROGRAM

Pub. L. 115–232, div. A, title XVI, §1641, Aug. 13, 2018, 132 Stat. 2131, provided that:

''(a) TRANSFER OF PROGRAM.—Not later than March 1, 2019, the Secretary of Defense shall transfer the operations and maintenance for the Sharkseer cybersecurity program from the National Security Agency to the Defense Information Systems Agency, including all associated funding and, as the Secretary considers necessary, personnel.

''(b) LIMITATION ON FUNDING FOR THE INFORMATION SYSTEMS SECURITY PROGRAM.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2019 or any subsequent fiscal year for research, development, test, and evaluation for the Information Systems Security Program for the National Security Agency, not more than 90 percent may be obligated or expended unless the Chief of Information Officer, in consultation with the Principal Cyber Advisor, certifies to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] that the operations and maintenance funding for the Sharkseer program for fiscal year 2019 and the subsequent fiscal years of the current Future Years Defense Program are available or programmed.

''(c) REPORT.—Not later than 90 days after the date of the enactment of this Act [Aug. 13, 2018], the Chief Information Officer shall provide to the congressional defense committees a report that assesses the transition of base operations of the SharkSeer program to the Defense Information Systems Agency, including with respect to staffing, acquisition, contracts, sensor management, and the ability to conduct cyber threat analyses and detect advanced malware. Such report shall also include a plan for continued capability development.

''(d) SHARKSEER BREAK AND INSPECT CAPABILITY.—

''(1) IN GENERAL.—The Secretary of Defense shall ensure that the decryption capability described in section 1636 of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291) [128 Stat. 3644] is provided by the break and inspect subsystem of the Sharkseer cybersecurity program, unless the Chief of Information Officer, in consultation with the Principal Cyber Advisor, notifies the congressional defense committees on or before the date that is 90 days after the date of the enactment of this Act that a superior enterprise solution will be operational before October 1, 2019.

''(2) INTEGRATION OF CAPABILITY.—The Secretary shall take such actions as are necessary to integrate the break and inspect subsystem of the Sharkseer cybersecurity program with the Department of Defense public key infrastructure.

''(e) VISIBILITY TO ENDPOINTS.—The Secretary shall take such actions as are necessary to enable, by October 1, 2020, the Sharkseer cybersecurity program and computer network defense service providers to instantly and automatically determine the specific identity and location of computer hosts and other endpoints that received or sent malware detected by the Sharkseer cybersecurity program or other network perimeter defenses.

''(f) SANDBOX AS A SERVICE.—The Secretary shall use the Sharkseer cybersecurity program sandbox-as-a-service capability as an enterprise solution and terminate all other such projects, unless the Chief of Information Officer, in consultation with the Principal Cyber Advisor, notifies the congressional defense com-

mittees on or before the date that is 90 days after the date of the enactment of this Act that a superior enterprise solution will be operational before October 1, 2019.''

DESIGNATION OF OFFICIAL FOR MATTERS RELATING TO INTEGRATING CYBERSECURITY AND INDUSTRIAL CONTROL SYSTEMS WITHIN THE DEPARTMENT OF DEFENSE

Pub. L. 115–232, div. A, title XVI, § 1643, Aug. 13, 2018, 132 Stat. 2133, provided that:

''(a) DESIGNATION OF INTEGRATING OFFICIAL.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall designate one official to be responsible for matters relating to integrating cybersecurity and industrial control systems for the Department of Defense.

''(b) RESPONSIBILITIES.—The official designated pursuant to subsection (a) shall be responsible for matters described in such subsection at all levels of command, from the Department's leadership to the facilities owned by or operated on behalf of the Department of Defense using industrial control systems, including developing Department-wide certification standards for integration of industrial control systems and taking into consideration frameworks set forth by the National Institute of Standards and Technology for the cybersecurity of such systems.''

ASSISTANCE FOR SMALL MANUFACTURERS IN THE DEFENSE INDUSTRIAL SUPPLY CHAIN AND UNIVERSITIES ON MATTERS RELATING TO CYBERSECURITY

Pub. L. 115–232, div. A, title XVI, § 1644, Aug. 13, 2018, 132 Stat. 2133, as amended by Pub. L. 116–283, div. A, title XVIII, §§ 1844(e)(2), 1869(e), Jan. 1, 2021, 134 Stat. 4246, 4284; Pub. L. 117–81, div. A, title XVII, § 1701(u)(5)(B), Dec. 27, 2021, 135 Stat. 2154, provided that:

''(a) DISSEMINATION OF CYBERSECURITY RESOURCES.—

''(1) IN GENERAL.—The Secretary of Defense, in consultation with the Director of the National Institute of Standards and Technology, shall take such actions as may be necessary to enhance awareness of cybersecurity threats among small manufacturers and universities working on Department of Defense programs and activities.

''(2) PRIORITY.—The Secretary of Defense shall prioritize efforts to increase awareness to help reduce cybersecurity risks faced by small manufacturers and universities referred to in paragraph (1).

''(3) SECTOR FOCUS.—The Secretary of Defense shall carry out this subsection with a focus on such small manufacturers and universities as the Secretary considers critical.

''(4) OUTREACH EVENTS.—Under paragraph (1), the Secretary of Defense shall conduct outreach to support activities consistent with this section. Such outreach may include live events with a physical presence and outreach conducted through Internet websites. Such outreach may include training, including via courses and classes, to help small manufacturers and universities improve their cybersecurity.

''(5) ROADMAPS AND ASSESSMENTS.—The Secretary of Defense shall ensure that cybersecurity for defense industrial base manufacturing is included in appropriate research and development roadmaps and threat assessments.

''(b) VOLUNTARY CYBERSECURITY SELF-ASSESSMENTS.—The Secretary of Defense shall develop mechanisms to provide assistance to help small manufacturers and universities conduct voluntary self-assessments in order to understand operating environments, cybersecurity requirements, and existing vulnerabilities, including through the Mentor Protégé Program, small business programs, and engagements with defense laboratories and test ranges.

''(c) TRANSFER OF RESEARCH FINDINGS AND EXPERTISE.—

''(1) IN GENERAL.—The Secretary of Defense shall promote the transfer of appropriate technology, threat information, and cybersecurity techniques developed in the Department of Defense to small manufacturers and universities throughout the United States to implement security measures that are adequate to protect covered defense information, including controlled unclassified information.

''(2) COORDINATION WITH OTHER FEDERAL EXPERTISE AND CAPABILITIES.—The Secretary of Defense shall coordinate efforts, when appropriate, with the expertise and capabilities that exist in Federal agencies and federally sponsored laboratories.

''(3) AGREEMENTS.—In carrying out this subsection, the Secretary of Defense may enter into agreements with private industry, institutes of higher education, or a State, United States territory, local, or tribal government to ensure breadth and depth of coverage to the United States defense industrial base and to leverage resources.

''(d) DEFENSE ACQUISITION WORKFORCE CYBER TRAINING PROGRAM.—The Secretary of Defense shall establish a cyber counseling certification program, or approve a similar existing program, to certify small business professionals and other relevant acquisition staff within the Department of Defense to provide cyber planning assistance to small manufacturers and universities.

''(e) ESTABLISHMENT OF CYBERSECURITY FOR DEFENSE INDUSTRIAL BASE MANUFACTURING ACTIVITY.—

''(1) AUTHORITY.—The Secretary of Defense may establish an activity to assess and strengthen the cybersecurity resiliency of the defense industrial base, if the Secretary determines such is appropriate.

''(2) DESIGNATION.—The activity described in paragraph (1), if established, shall be known as the 'Cybersecurity for Defense Industrial Base Manufacturing Activity'.

''(3) SPECIFICATION.—The Cybersecurity for Defense Industrial Base Manufacturing Activity, if established, shall implement the requirements specified in subsections (a) through (c).

''(f) AUTHORITIES.—In carrying out this section, the Secretary may use the following authorities:

''(1) The Manufacturing Technology Program established under section 4841 of title 10, United States Code.

''(2) The Centers for Science, Technology, and Engineering Partnership program under section 2368 of title 10, United States Code [now 10 U.S.C. 4124].

''(3) The Manufacturing Engineering Education Program established under section 2196 of title 10, United States Code [now 10 U.S.C. 4843].

''(4) The Small Business Innovation Research program.

''(5) The mentor-protégé program.

''(6) Other legal authorities as the Secretary determines necessary to effectively and efficiently carry out this section.

''(g) DEFINITIONS.—In this section:

''(1) RESOURCES.—The term 'resources' means guidelines, tools, best practices, standards, methodologies, and other ways of providing information.

''(2) SMALL BUSINESS CONCERN.—The term 'small business concern' means a small business concern as that term is used in section 3 of the Small Business Act (15 U.S.C. 632).

''(3) SMALL MANUFACTURER.—The term 'small manufacturer' means a small business concern that is a manufacturer in the defense industrial supply chain.

''(4) STATE.—The term 'State' means each of the several States, Territories, and possessions of the United States, the District of Columbia, and the Commonwealth of Puerto Rico.''

EMAIL AND INTERNET WEBSITE SECURITY AND AUTHENTICATION

Pub. L. 115–232, div. A, title XVI, § 1645, Aug. 13, 2018, 132 Stat. 2135, provided that:

''(a) IMPLEMENTATION OF PLAN REQUIRED.—Except as provided by subsection (b), the Secretary of Defense shall develop and implement the plan outlined in Binding Operational Directive 18–01, issued by the Secretary

of Homeland Security on October 16, 2017, relating to email security and authentication and Internet website security, according to the schedule established by the Binding Operational Directive for the rest of the Executive Branch beginning with the date of enactment of this Act [Aug. 13, 2018].

''(b) WAIVER.—The Secretary may waive the requirements of subsection (a) if the Secretary submits to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Committee on Oversight and Government Reform [now Committee on Oversight and Accountability] of the House of Representatives, and the Committee on Homeland Security and Government Affairs of the Senate a certification that existing or planned security measures for the Department of Defense either meet or exceed the information security requirements of Binding Operational Directive 18–01.

''(c) FUTURE BINDING OPERATIONAL DIRECTIVES.—The Chief Information Officer of the Department of Defense shall notify the congressional defense committees, the Committee on Oversight and Government Reform [now Committee on Oversight and Accountability] of the House of Representatives, and the Committee on Homeland Security and Government Affairs of the Senate within 180 days of the issuance by the Secretary of Homeland Security after the date of the enactment of this Act of any Binding Operational Directive for cybersecurity whether the Department of Defense will comply with the Directive or how the Department of Defense plans to meet or exceed the security objectives of the Directive.''

RISK THRESHOLDS FOR SYSTEMS AND NETWORK OPERATIONS

Pub. L. 115–232, div. A, title XVI, §1647(c), Aug. 13, 2018, 132 Stat. 2136, provided that: ''The Chief Information Officer of the Department of Defense, in coordination with the Principal Cyber Advisor, the Director of Operations of the Joint Staff, and the Commander of United States Cyber Command, shall establish risk thresholds for systems and network operations that, when exceeded, would trigger heightened security measures, such as enhanced monitoring and access policy changes.''

MITIGATION OF RISKS TO NATIONAL SECURITY POSED BY PROVIDERS OF INFORMATION TECHNOLOGY PRODUCTS AND SERVICES WHO HAVE OBLIGATIONS TO FOREIGN GOVERNMENTS

Pub. L. 115–232, div. A, title XVI, §1655, Aug. 13, 2018, 132 Stat. 2149, provided that:

''(a) DISCLOSURE REQUIRED.—Subject to the regulations issued under subsection (b), the Department of Defense may not use a product, service, or system procured or acquired after the date of the enactment of this Act [Aug. 13, 2018] relating to information or operational technology, cybersecurity, an industrial control system, or weapons system provided by a person unless that person discloses to the Secretary of Defense the following:

''(1) Whether, and if so, when, within five years before or at any time after the date of the enactment of this Act, the person has allowed a foreign government to review the code of a non-commercial product, system, or service developed for the Department, or whether the person is under any obligation to allow a foreign person or government to review the code of a non-commercial product, system, or service developed for the Department as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government.

''(2) Whether, and if so, when, within five years before or at any time after the date of the enactment of this Act, the person has allowed a foreign government listed in section 1654 [of Pub. L. 115–232, 10 U.S.C. 394 note] to review the source code of a product, system, or service that the Department is using or intends to use, or is under any obligation to allow a foreign person or government to review the source code of a product, system, or service that the Department is using or intends to use as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government.

''(3) Whether or not the person holds or has sought a license pursuant to the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations, or successor regulations, for information technology products, components, software, or services that contain code custom-developed for the non-commercial product, system, or service the Department is using or intends to use.

''(b) REGULATIONS.—

''(1) IN GENERAL.—The Secretary of Defense shall issue regulations regarding the implementation of subsection (a).

''(2) UNIFORM REVIEW PROCESS.—If information obtained from a person under subsection (a) or the contents of the registry under subsection (f) are the subject of a request under section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act'), the Secretary of Defense shall conduct a uniform review process, without regard to the office holding the information, to determine if the information is exempt from disclosure under such section 552.

''(c) PROCUREMENT.—Procurement contracts for covered products or systems shall include a clause requiring the information contained in subsection (a) be disclosed during the period of the contract if an entity becomes aware of information requiring disclosure required pursuant to such subsection, including any mitigation measures taken or anticipated.

''(d) MITIGATION OF RISKS.—

''(1) IN GENERAL.—If, after reviewing a disclosure made by a person under subsection (a), the Secretary determines that the disclosure relating to a product, system, or service entails a risk to the national security infrastructure or data of the United States, or any national security system under the control of the Department, the Secretary shall take such measures as the Secretary considers appropriate to mitigate such risks, including, as the Secretary considers appropriate, by conditioning any agreement for the use, procurement, or acquisition of the product, system, or service on the inclusion of enforceable conditions or requirements that would mitigate such risks.

''(2) THIRD-PARTY TESTING STANDARD.—Not later than two years after the date of the enactment of this Act the Secretary shall develop such third-party testing standard as the Secretary considers acceptable for commercial off the shelf (COTS) products, systems, or services to use when dealing with foreign governments.

''(e) EXEMPTION OF OPEN SOURCE SOFTWARE.—This section shall not apply to open source software.

''(f) ESTABLISHMENT OF REGISTRY.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall—

''(1) establish within the operational capabilities of the Committee for National Security Systems (CNSS) or within such other agency as the Secretary considers appropriate a registry containing the information disclosed under subsection (a); and

''(2) upon request, make such information available to any agency conducting a procurement pursuant to the Federal Acquisition Regulations or the Defense Federal Acquisition Regulations.

''(g) ANNUAL REPORTS.—Not later than one year after the date of the enactment of this Act and not less frequently than once each year thereafter, the Secretary of Defense shall submit to the appropriate committees of Congress a report detailing the number, scope, prod-

uct classifications, and mitigation agreements related to each product, system, and service for which a disclosure is made under subsection (a).

''(h) DEFINITIONS.—In this section:

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

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

''(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Oversight and Government Reform [now Committee on Oversight and Accountability] of the House of Representatives.

''(2) COMMERCIAL ITEM.—The term 'commercial item' has the meaning given such term in section 103 of title 41, United States Code.

''(3) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given such term in section 11101 of title 40, United States Code.

''(4) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given such term in section 3552(b) of title 44, United States Code.

''(5) NON-COMMERCIAL PRODUCT, SYSTEM, OR SERVICE.—The term 'non-commercial product, system, or service' means a product, system, or service that does not meet the criteria of a commercial item.

''(6) OPEN SOURCE SOFTWARE.—The term 'open source software' means software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software.''

INTEGRATION OF STRATEGIC INFORMATION OPERATIONS AND CYBER-ENABLED INFORMATION OPERATIONS

Pub. L. 115–91, div. A, title XVI, §1637, Dec. 12, 2017, 131 Stat. 1742, provided that:

''(a) PROCESSES AND PROCEDURES FOR INTEGRATION.—

''(1) IN GENERAL.—The Secretary of Defense shall—

''(A) establish processes and procedures to integrate strategic information operations and cyber-enabled information operations across the elements of the Department of Defense responsible for such operations, including the elements of the Department responsible for military deception, public affairs, electronic warfare, and cyber operations; and

''(B) ensure that such processes and procedures provide for integrated Defense-wide strategy, planning, and budgeting with respect to the conduct of such operations by the Department, including activities conducted to counter and deter such operations by malign actors.

''(2) DESIGNATED SENIOR OFFICIAL.—The Secretary of Defense shall designate a senior official of the Department of Defense (in this section referred to as the 'designated senior official') who shall implement and oversee the processes and procedures established under paragraph (1). The designated senior official shall be selected by the Secretary from among individuals serving in the Department of Defense at or below the level of an Under Secretary of Defense.

''(3) RESPONSIBILITIES.—The designated senior official shall have, with respect to the implementation and oversight of the processes and procedures established under paragraph (1), the following responsibilities:

''(A) Oversight of strategic policy and guidance.

''(B) Overall resource management for the integration of information operations and cyber-enabled information operations of the Department.

''(C) Coordination with the head of the Global Engagement Center to support the purpose of the Center (as described [in] section 1287(a)(2) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note)) and liaison with the Center and other relevant Federal Government entities to support such purpose.

''(D) Development of a strategic framework for the conduct of information operations by the Department of Defense, including cyber-enabled information operations, coordinated across all relevant elements of the Department of Defense, including both near-term and long-term guidance for the conduct of such coordinated operations.

''(E) Development and dissemination of a common operating paradigm across the elements of the Department of Defense specified in paragraph (1) to counter the influence, deception, and propaganda activities of key malign actors, including in cyberspace.

''(F) Development of guidance for, and promotion of, the capability of the Department of Defense to liaison with the private sector, including social media, on matters relating to the influence activities of malign actors.

''(b) REQUIREMENTS AND PLANS FOR INFORMATION OPERATIONS.—

''(1) COMBATANT COMMAND PLANNING AND REGIONAL STRATEGY.—(A) The Secretary shall require each commander of a combatant command to develop, in coordination with the relevant regional Assistant Secretary of State or Assistant Secretaries of State and with the assistance of the Coordinator of the Global Engagement Center and the designated senior official, a regional information strategy and interagency coordination plan for carrying out the strategy, where applicable.

''(B) The Secretary shall require each commander of a combatant command to develop such requirements and specific plans as may be necessary for the conduct of information operations in support of the strategy required under subparagraph (A), including plans for deterring information operations, including deterrence in the cyber domain, by malign actors against the United States, allies of the United States, and interests of the United States.

''(2) IMPLEMENTATION PLAN FOR DOD STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT.—

''(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the designated senior official shall—

''(i) review the strategy of the Department of Defense titled 'Department of Defense Strategy for Operations in the Information Environment' and dated June 2016; and

''(ii) submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for implementation of such strategy.

''(B) ELEMENTS.—The plan required under subparagraph (A) shall include, at a minimum, the following:

''(i) An accounting of the efforts undertaken in support of the strategy described in subparagraph (A)(i) in the period since it was issued in June 2016.

''(ii) A description of any updates or changes to such strategy that have been made since it was first issued, as well as any expected updates or changes resulting from the designation of the designated senior official.

''(iii) A description of the role of the Department of Defense as part of a broader whole-of-Government strategy for strategic communications, including a description of any assumptions about the roles and contributions of other departments and agencies of the Federal Government with respect to such a strategy.

''(iv) Defined actions, performance metrics, and projected timelines for achieving each of the 15 tasks specified in the strategy described in subparagraph (A)(i).

''(v) An analysis of any personnel, resourcing, capability, authority, or other gaps that will need to be addressed to ensure effective implementation of the strategy described in subparagraph

(A)(i) across all relevant elements of the Department of Defense.

''(vi) An investment framework and projected timeline for addressing any gaps identified under clause (v).

''(vii) Such other matters as the Secretary of Defense considers relevant.

''(C) PERIODIC STATUS REPORTS.—Not less frequently than once every 90 days during the three-year period beginning on the date on which the implementation plan is submitted under subparagraph (A)(ii), the designated senior official shall submit to the congressional defense committees a report describing the status of the efforts of the Department of Defense in accomplishing the tasks specified under clauses (iv) and (vi) of subparagraph (B).

''(c) TRAINING AND EDUCATION.—Consistent with the elements of the implementation plan under paragraph (2), the designated senior official shall recommend the establishment of programs to provide training and education to such members of the Armed Forces and civilian employees of the Department of Defense as the Secretary considers appropriate to ensure that such members and employees understand the role of information in warfare, the central goal of all military operations to affect the perceptions, views, and decision making of adversaries, and the effective management and conduct of operations in the information environment.''

EXERCISE ON ASSESSING CYBERSECURITY SUPPORT TO ELECTION SYSTEMS OF STATES

Pub. L. 115–91, div. A, title XVI, §1638, Dec. 12, 2017, 131 Stat. 1744, provided that:

''(a) INCLUSION OF CYBER VULNERABILITIES IN ELECTION SYSTEMS IN CYBER GUARD EXERCISES.—Subject to subsection (b), the Secretary of Defense, in consultation with the Secretary of Homeland Security, may carry out exercises relating to the cybersecurity of election systems of States as part of the exercise commonly known as the 'Cyber Guard Exercise'.

''(b) AGREEMENT REQUIRED.—The Secretary of Defense may carry out an exercise relating to the cybersecurity of a State's election system under subsection (a) only if the State enters into a written agreement with the Secretary under which the State—

''(1) agrees to participate in such exercise; and

''(2) agrees to allow vulnerability testing of the components of the State's election system.

''(c) REPORT.—Not later than 90 days after the completion of any Cyber Guard Exercise, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the ability of the National Guard to assist States, if called upon, in defending election systems from cyberattacks. Such report shall include a description of the capabilities, readiness levels, and best practices of the National Guard with respect to the prevention of cyber attacks on State election systems.''

MEASUREMENT OF COMPLIANCE WITH CYBERSECURITY REQUIREMENTS FOR INDUSTRIAL CONTROL SYSTEMS

Pub. L. 115–91, div. A, title XVI, §1639, Dec. 12, 2017, 131 Stat. 1744, provided that:

''(a) IN GENERAL.—Not later than January 1, 2018, the Secretary of Defense shall make such changes to the cybersecurity scorecard as are necessary to ensure that the Secretary measures the progress of each element of the Department of Defense in securing the industrial control systems of the Department against cyber threats, including such industrial control systems as supervisory control and data acquisition systems, distributed control systems, programmable logic controllers, and platform information technology.

''(b) CYBERSECURITY SCORECARD DEFINED.—In this section, the term 'cybersecurity scorecard' means the Department of Defense Cybersecurity Scorecard used by the Department to measure compliance with cybersecurity requirements as described in the plan of the Department titled 'Department of Defense Cybersecurity Discipline Implementation Plan'.''

STRATEGIC CYBERSECURITY PROGRAM

Pub. L. 115–91, div. A, title XVI, §1640, Dec. 12, 2017, 131 Stat. 1745, as amended by Pub. L. 116–283, div. A, title XVII, §1712(b), Jan. 1, 2021, 134 Stat. 4087; Pub. L. 117–81, div. A, title XV, §1525, Dec. 27, 2021, 135 Stat. 2043; Pub. L. 117–263, div. A, title XV, §1503, Dec. 23, 2022, 136 Stat. 2880, which provided for the establishment of the Strategic Cybersecurity Program to ensure the Department of Defense's ability to conduct the most important military missions of the Department, was repealed by Pub. L. 118–31, div. A, title XV, §1502(a)(2)(C), Dec. 22, 2023, 137 Stat. 537. See section 391b of this title.

REQUIREMENT TO ENTER INTO AGREEMENTS RELATING TO USE OF CYBER OPPOSITION FORCES

Pub. L. 114–328, div. A, title XVI, §1644, Dec. 23, 2016, 130 Stat. 2602, provided that:

''(a) REQUIREMENT FOR AGREEMENTS.—Not later than September 30, 2017, the Secretary of Defense shall ensure that each commander of a combatant command establishes appropriate agreements with the Secretary relating to the use of cyber opposition forces. Each agreement shall require the command—

''(1) to support a high state of mission readiness in the command through the use of one or more cyber opposition forces in continuous exercises and other training activities as considered appropriate by the commander of the command; and

''(2) in conducting such exercises and training activities, [to] meet the standard required under subsection (b).

''(b) JOINT STANDARD FOR CYBER OPPOSITION FORCES.—Not later than March 31, 2017, the Secretary of Defense shall issue a joint training and certification standard for use by all cyber opposition forces within the Department of Defense.

''(c) JOINT STANDARD FOR PROTECTION OF CONTROL SYSTEMS.—Not later than June 30, 2017, the Secretary of Defense shall issue a joint training and certification standard for the protection of control systems for use by all cyber operations forces within the Department of Defense. Such standard shall—

''(1) provide for applied training and exercise capabilities; and

''(2) use expertise and capabilities from other departments and agencies of the Federal Government, as appropriate.

''(d) BRIEFING REQUIRED.—Not later than September 30, 2017, the Secretary of Defense shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing that includes—

''(1) a list of each combatant command that has established an agreement under subsection (a);

''(2) with respect to each such agreement—

''(A) special conditions in the agreement placed on any cyber opposition force used by the command;

''(B) the process for making decisions about deconfliction and risk mitigation of cyber opposition force activities in continuous exercises and training;

''(C) identification of cyber opposition forces trained and certified to operate at the joint standard, as issued under subsection (b);

''(D) identification of the annual exercises that will include participation of the cyber opposition forces; and

''(E) identification of any shortfalls in resources that may prevent annual exercises using cyber opposition forces; and

''(3) any other matters the Secretary of Defense considers appropriate.''

CYBER PROTECTION SUPPORT FOR DEPARTMENT OF DEFENSE PERSONNEL IN POSITIONS HIGHLY VULNERABLE TO CYBER ATTACK

Pub. L. 114–328, div. A, title XVI, §1645, Dec. 23, 2016, 130 Stat. 2603, provided that:

''(a) AUTHORITY TO PROVIDE CYBER PROTECTION SUPPORT.—

''(1) IN GENERAL.—Subject to a determination by the Secretary of Defense, the Secretary may provide cyber protection support for the personal technology devices of the personnel described in paragraph (2).

''(2) AT-RISK PERSONNEL.—The personnel described in this paragraph are personnel of the Department of Defense—

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

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

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

''(c) LIMITATION ON SUPPORT.—Nothing in this section shall be construed—

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

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

''(d) REPORT.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the provision of cyber protection support under subsection (a). The report shall include—

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

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

''(e) PERSONAL TECHNOLOGY DEVICES DEFINED.—In this section, the term 'personal technology devices' means technology devices used by Department of Defense personnel outside of the scope of their employment with the Department and includes networks to which such devices connect.''

LIMITATION ON FULL DEPLOYMENT OF JOINT REGIONAL SECURITY STACKS

Pub. L. 114–328, div. A, title XVI, §1646, Dec. 23, 2016, 130 Stat. 2604, provided that:

''(a) LIMITATION.—The Secretary of a military department or the head of a Defense Agency may not declare that such department or Defense Agency has achieved full operational capability for the deployment of joint regional security stacks until the date on which—

''(1) the department or Defense Agency concerned completes operational test and evaluation activities to determine the effectiveness, suitability, and survivability of the joint regional security stacks system of such department or Defense Agency; and

''(2) written certification that such testing and evaluation activities have been completed is provided to the Secretary of such department or the head of such Defense Agency by the appropriate operational test and evaluation organization of such department or Defense Agency.

''(b) WAIVER.—

''(1) IN GENERAL.—The Secretary of a military department or the head of a Defense Agency may waive the requirements of subsection (a) if a certification described in paragraph (2) is provided to the Secretary of Defense, and signed by—

''(A) the Secretary of the military department or the head of the Defense Agency concerned;

''(B) the Director of Operational Test and Evaluation for the Department of Defense; and

''(C) the Chief Information Officer of the Department of Defense.

''(2) CERTIFICATION.—A certification described in this subsection is a written certification that—

''(A) the testing and evaluation activities required under subsection (a) are unnecessary, accompanied by an explanation of the reasons such activities are unnecessary;

''(B) the effectiveness, suitability, and survivability of the joint regional security stacks system of the military department or Defense Agency concerned has been demonstrated by methods other than the testing and evaluation activities required under subsection (a), accompanied by supporting data; or

''(C) national security needs justify full deployment of the joint regional security stacks system of the military department or Defense Agency concerned before the test and evaluation activities required under subsection (a) can be completed, accompanied by an explanation of such justification and a risk management plan.''

EVALUATION OF CYBER VULNERABILITIES OF DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE

Pub. L. 114–328, div. A, title XVI, §1650, Dec. 23, 2016, 130 Stat. 2607, as amended by Pub. L. 115–91, div. A, title XVI, §1643, Dec. 12, 2017, 131 Stat. 1748; Pub. L. 115–232, div. A, title XVI, §1634, Aug. 13, 2018, 132 Stat. 2125; Pub. L. 118–31, div. A, title XV, §1502(a)(2)(B), Dec. 22, 2023, 137 Stat. 537, provided that:

''(a) PLAN FOR EVALUATION.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for the evaluation of the cyber vulnerabilities of the critical infrastructure of the Department of Defense.

''(2) ELEMENTS.—The plan under paragraph (1) shall include—

''(A) an identification of each of the military installations to be evaluated; and

''(B) an estimate of the cost of the evaluation.

''(3) PRIORITY IN EVALUATION.—The plan under paragraph (1) shall prioritize the evaluation of military installations based on the criticality of the infrastructure supporting such installations, as determined by the Chairman of the Joint Chiefs of Staff based on an assessment of—

''(A) the Armed Forces stationed at such military installations; and

''(B) threats to such military installations.

''(4) INTEGRATION WITH OTHER EFFORTS.—The plan under paragraph (1) shall build upon other efforts of Department of Defense relating to the identification and mitigation of cyber vulnerabilities of major weapon systems and critical infrastructure of the Department and shall not duplicate such efforts.

''(b) PILOT PROGRAM.—

''(1) IN GENERAL.—Not later than 30 days after the date on which the Secretary submits the plan under subsection (a), the Secretary, acting through a covered research laboratory and the Defense Digital Service, shall initiate a pilot program under which the Secretary shall assess the feasibility and advisability of applying new, innovative methodologies or engineering approaches—

''(A) to improve the defense of control systems against cyber attacks;

''(B) to increase the resilience of military installations against cybersecurity threats;

''(C) to prevent or mitigate the potential for high-consequence cyber attacks;

''(D) to inform future requirements for the development of such control systems; and

''(E) to assess the strategic benefits derived from, and the challenges associated with, isolating military infrastructure from the national electric grid and the use of microgrids.

''(2) LOCATIONS.—The Secretary shall carry out the pilot program under paragraph (1) at not fewer than

two military installations selected by the Secretary from among military installations that support the most critical mission-essential functions of the Department of Defense as identified in the plan under subsection (a).

''(3) TOOLS.—In carrying out the pilot program under paragraph (1), the Secretary may use tools and solutions developed under subsection (e).

''(4) REPORT.—Not later than December 31, 2020, the Secretary shall submit to the congressional defense committees a final report on the pilot program that includes—

''(A) a description of the activities carried out under the pilot program at each military installation concerned;

''(B) an assessment of the value of the methodologies or tools applied during the pilot program in increasing the resilience of military installations against cybersecurity threats;

''(C) recommendations for administrative or legislative actions to improve the ability of the Department to employ methodologies and tools for reducing cyber vulnerabilities in other activities of the Department of Defense; and

''(D) recommendations for including such methodologies or tools as requirements for relevant activities, including technical requirements for systems or military construction projects.

''(5) TERMINATION.—The authority of the Secretary to carry out the pilot program under this subsection shall terminate on September 30, 2020.

''(c) EVALUATION.—

''(1) IN GENERAL.—Not later than December 31, 2020, the Secretary shall complete an evaluation of the cyber vulnerabilities of the critical infrastructure of the Department of Defense in accordance with the plan under subsection (a).

''(2) RISK MITIGATION STRATEGIES.—The Secretary shall develop strategies for mitigating the risks of cyber vulnerabilities identified in the course of the evaluation under paragraph (1).

''(d) TOOLS AND SOLUTIONS.—The Secretary may—

''(1) develop tools that improve assessments of cyber vulnerabilities of Department of Defense critical infrastructure;

''(2) conduct non-recurring engineering for the design of mitigation solutions for such vulnerabilities; and

''(3) establish Department-wide information repositories to share findings relating to such assessments and to share such mitigation solutions.

''(e) DEFINITIONS.—In this section:

''(1) CRITICAL INFRASTRUCTURE OF THE DEPARTMENT OF DEFENSE.—The term 'critical infrastructure of the Department of Defense' means any asset of the Department of Defense of such extraordinary importance to the functioning of the Department and the operation of the Armed Forces that the incapacitation or destruction of such asset by a cyber attack would have a debilitating effect on the ability of the Department to fulfill its missions.

''(2) COVERED RESEARCH LABORATORY.—The term 'covered research laboratory' means—

''(A) a research laboratory of the Department of Defense; or

''(B) a research laboratory of the Department of Energy approved by the Secretary of Energy to carry out the pilot program under subsection (b).''

PLAN FOR INFORMATION SECURITY CONTINUOUS MONITORING CAPABILITY AND COMPLY-TO-CONNECT POLICY; LIMITATION ON SOFTWARE LICENSING

Pub. L. 114–328, div. A, title XVI, §1653, Dec. 23, 2016, 130 Stat. 2610, provided that:

''(a) INFORMATION SECURITY MONITORING PLAN AND POLICY.—

''(1) PLAN AND POLICY.—The Chief Information Officer of the Department of Defense and the Commander of the United States Cyber Command shall jointly develop—

''(A) a plan for a modernized, Department-wide automated information security continuous monitoring capability that includes—

''(i) a proposed information security architecture for the capability;

''(ii) a concept of operations for the capability; and

''(iii) requirements with respect to the functionality and interoperability of the tools, sensors, systems, processes, and other components of the continuous monitoring capability; and

''(B) a comply-to-connect policy that requires systems to automatically comply with the configurations of the networks of the Department as a condition of connecting to such networks.

''(2) CONSULTATION.—In developing the plan and policy under paragraph (1), the Chief Information Officer and the Commander shall consult with the Principal Cyber Advisor to the Secretary of Defense.

''(3) IMPLEMENTATION.—The Chief Information Officer and the Commander shall each issue such directives as they each consider appropriate to ensure compliance with the plan and policy developed under paragraph (1).

''(4) INCLUSION IN BUDGET MATERIALS.—The Secretary of Defense shall include funding and program plans relating to the plan and policy under paragraph (1) in the budget materials submitted by the Secretary in support of the budget of the President for fiscal year 2019 (as submitted to Congress under section 1105(a) of title 31, United States Code).

''(5) INTEGRATION WITH OTHER CAPABILITIES.—The Chief Information Officer and the Commander shall ensure that information generated through automated and automation-assisted processes for continuous monitoring, asset management, and comply-to-connect policies and processes shall be accessible and usable in machine-readable form to appropriate cyber protection teams and computer network defense service providers.

''(6) SOFTWARE LICENSE COMPLIANCE MATTERS.—The plan and policy required by paragraph (1) shall comply with the software license inventory requirements of the plan issued pursuant to section 937 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2223 note) and updated pursuant to section 935 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 10 U.S.C. 2223 note).

''(b) LIMITATION ON FUTURE SOFTWARE LICENSING.—

''(1) IN GENERAL.—Subject to paragraph (2), none of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2017 or any fiscal year thereafter for the Department of Defense may be obligated or expended on a contract for a software license with a cost of more than $5,000,000 in a fiscal year unless the Department is able, through automated means—

''(A) to count the number of such licenses in use; and

''(B) to determine the security status of each instance of use of the software licensed.

''(2) EFFECTIVE DATE.—Paragraph (1) shall apply—

''(A) beginning on January 1, 2018, with respect to any contract entered into by the Secretary of Defense on or after such date for the licensing of software; and

''(B) beginning on January 1, 2020, with respect to any contract entered into by the Secretary for the licensing of software that was in effect on December 31, 2017.''

ACQUISITION AUTHORITY OF THE COMMANDER OF UNITED STATES CYBER COMMAND

Pub. L. 114–92, div. A, title VIII, §807, Nov. 25, 2015, 129 Stat. 886, as amended by Pub. L. 115–232, div. A, title XVI, §1635, Aug. 13, 2018, 132 Stat. 2125; Pub. L. 116–92, div. A, title VIII, §821, Dec. 20, 2019, 133 Stat. 1490; Pub. L. 116–283, div. A, title XVII, §1711, Jan. 1, 2021, 134 Stat. 4086, provided that:

''(a) AUTHORITY.—

''(1) IN GENERAL.—The Commander of the United States Cyber Command shall be responsible for, and shall have the authority to conduct, the following acquisition activities:

''(A) Development and acquisition of cyber operations-peculiar equipment and capabilities.

''(B) Acquisition and sustainment of cyber capability-peculiar equipment, capabilities, and services.

''(2) ACQUISITION FUNCTIONS.—Subject to the authority, direction, and control of the Secretary of Defense, the Commander shall have authority to exercise the functions of the head of an agency under chapter 137 of title 10, United States Code.

''(b) COMMAND ACQUISITION EXECUTIVE.—

''(1) IN GENERAL.—The staff of the Commander shall include a command acquisition executive, who shall be responsible for the overall supervision of acquisition matters for the United States Cyber Command. The command acquisition executive shall have the authority—

''(A) to negotiate memoranda of agreement with the military departments and Department of Defense components to carry out the acquisition of equipment, capabilities, and services described in subsection (a)(1) on behalf of the Command;

''(B) to supervise the acquisition of equipment, capabilities, and services described in subsection (a)(1);

''(C) to represent the Command in discussions with the military departments regarding acquisition programs for which the Command is a customer; and

''(D) to work with the military departments to ensure that the Command is appropriately represented in any joint working group or integrated product team regarding acquisition programs for which the Command is a customer.

''(2) DELIVERY OF ACQUISITION SOLUTIONS.—The command acquisition executive of the United States Cyber Command shall be—

''(A) responsible to the Commander for rapidly delivering acquisition solutions to meet validated cyber operations-peculiar requirements;

''(B) subordinate to the defense acquisition executive in matters of acquisition;

''(C) subject to the same oversight as the service acquisition executives; and

''(D) included on the distribution list for acquisition directives and instructions of the Department of Defense.

''(c) ACQUISITION PERSONNEL.—

''(1) IN GENERAL.—The Secretary of Defense shall provide the United States Cyber Command with the personnel or funding equivalent to ten full-time equivalent personnel to support the Commander in fulfilling the acquisition responsibilities provided for under this section with experience in—

''(A) program acquisition;

''(B) the Joint Capabilities Integration and Development System Process;

''(C) program management;

''(D) system engineering; and

''(E) costing.

''(2) EXISTING PERSONNEL.—The personnel provided under this subsection shall be provided from among the existing personnel of the Department of Defense.

''(d) BUDGET.—In addition to the activities of a combatant command for which funding may be requested under section 166 of title 10, United States Code, the budget proposal of the United States Cyber Command shall include requests for funding for—

''(1) development and acquisition of cyber operations-peculiar equipment; and

''(2) acquisition and sustainment of other capabilities or services that are peculiar to cyber operations activities.

''(e) RULE OF CONSTRUCTION REGARDING INTELLIGENCE AND SPECIAL ACTIVITIES.—Nothing in this section shall be construed to constitute authority to conduct any activity which, if carried out as an intelligence activity by the Department of Defense, would require a notice to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.).

''(f) IMPLEMENTATION PLAN REQUIRED.—The authority granted in subsection (a) shall become effective 30 days after the date on which the Secretary of Defense provides to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for implementation of those authorities under subsection (a). The plan shall include the following:

''(1) A Department of Defense definition of—

''(A) cyber operations-peculiar equipment and capabilities; and

''(B) cyber capability-peculiar equipment, capabilities, and services.

''(2) Summaries of the components to be negotiated in the memorandum of agreements with the military departments and other Department of Defense components to carry out the development, acquisition, and sustainment of equipment, capabilities, and services described in subparagraphs (A) and (B) of subsection (a)(1).

''(3) Memorandum of agreement negotiation and approval timelines.

''(4) Plan for oversight of the command acquisition executive established in subsection (b).

''(5) Assessment of the acquisition workforce needs of the United States Cyber Command to support the authority in subsection (a) until 2021.

''(6) Other matters as appropriate.

''(g) ANNUAL END-OF-YEAR ASSESSMENT.—Each year, the Cyber Investment Management Board shall review and assess the acquisition activities of the United States Cyber Command, including contracting and acquisition documentation, for the previous fiscal year, and provide any recommendations or feedback to the acquisition executive of Cyber Command.''

EVALUATION OF CYBER VULNERABILITIES OF MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE

Pub. L. 114–92, div. A, title XVI, §1647, Nov. 25, 2015, 129 Stat. 1118, as amended by Pub. L. 114–328, div. A, title XVI, §1649(b), Dec. 23, 2016, 130 Stat. 2606; Pub. L. 116–92, div. A, title XVI, §1633, Dec. 20, 2019, 133 Stat. 1746; Pub. L. 116–283, div. A, title XVII, §1712(a), Jan. 1, 2021, 134 Stat. 4087; Pub. L. 118–31, div. A, title XV, §1502(a)(2)(A), Dec. 22, 2023, 137 Stat. 537, provided that:

''(a) EVALUATION REQUIRED.—

''(1) IN GENERAL.—The Secretary of Defense shall, in accordance with the plan under subsection (b), complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department of Defense by not later than December 31, 2019.

''(2) EXCEPTION.—The Secretary may waive the requirement of paragraph (1) with respect to a weapon system or complete the evaluation of a weapon system required by such paragraph after the date specified in such paragraph if the Secretary certifies to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] before that date that all known cyber vulnerabilities in the weapon system have minimal consequences for the capability of the weapon system to meet operational requirements or otherwise satisfy mission requirements.

''(b) PLAN FOR EVALUATION.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Nov. 25, 2015], the Secretary shall submit to the congressional defense committees the plan of the Secretary for the evaluations of major weapon systems under subsection (a), including an identification of each of the weapon systems to be evaluated and an estimate of the funding required to conduct the evaluations.

''(2) PRIORITY IN EVALUATIONS.—The plan under paragraph (1) shall accord a priority among evalua-

tions based on the criticality of major weapon systems, as determined by the Chairman of the Joint Chiefs of Staff based on an assessment of employment of forces and threats.

''(3) INTEGRATION WITH OTHER EFFORTS.—The plan under paragraph (1) shall build upon existing efforts regarding the identification and mitigation of cyber vulnerabilities of major weapon systems, and shall not duplicate similar ongoing efforts such as Task Force Cyber Awakening of the Navy or Task Force Cyber Secure of the Air Force.

''(c) TOOLS AND SOLUTIONS FOR ASSESSING AND MITIGATING CYBER VULNERABILITIES.—In addition to carrying out the evaluation of cyber vulnerabilities of major weapon systems of the Department under this section, the Secretary may—

''(1) develop tools to improve the detection and evaluation of cyber vulnerabilities;

''(2) conduct non-recurring engineering for the design of solutions to mitigate cyber vulnerabilities; and

''(3) establish Department-wide information repositories to share findings relating to the evaluation and mitigation of cyber vulnerabilities.

''(d) RISK MITIGATION STRATEGIES.—As part of the evaluation of cyber vulnerabilities of major weapon systems of the Department under this section, the Secretary shall develop strategies for mitigating the risks of cyber vulnerabilities identified in the course of such evaluations.

''(e) AUTHORIZATION OF APPROPRIATIONS.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2016 for research, development, test, and evaluation, Defense-wide, not more than $200,000,000 shall be available to the Secretary to conduct the evaluations under subsection (a)(1).

''(f) WRITTEN NOTIFICATION.—If the Secretary determines that the Department will not complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department by the date specified in subsection (a)(1), the Secretary shall provide to the congressional defense committees written notification relating to each such incomplete evaluation. Such a written notification shall include the following:

''(1) An identification of each major weapon system for which an evaluation will not be complete by the date specified in subsection (a)(1), the anticipated date of completion of the evaluation of each such weapon system, and a description of the remaining work to be done for the evaluation of each such weapon system.

''(2) A justification for the inability to complete such an evaluation by the date specified in subsection (a)(1).

''(g) REPORT.—The Secretary, acting through the Under Secretary of Defense for Acquisition and Sustainment, shall provide a report to the congressional defense committees upon completion of the requirement for an evaluation of the cyber vulnerabilities of each major weapon system of the Department under this section. Such report shall include the following:

''(1) An identification of cyber vulnerabilities of each major weapon system requiring mitigation.

''(2) An identification of current and planned efforts to address the cyber vulnerabilities of each major weapon system requiring mitigation, including efforts across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities of the Department.

''(3) A description of joint and common cyber vulnerability mitigation solutions and efforts, including solutions and efforts across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities of the Department.

''(4) A description of lessons learned and best practices regarding evaluations of the cyber vulnerabilities and cyber vulnerability mitigation efforts relating to major weapon systems, including an identification of useful tools and technologies for discovering and mitigating vulnerabilities, such as those specified in section 1657 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) [132 Stat. 2151], and steps taken to institutionalize the use of these tools and technologies.

''(5) A description of efforts to share lessons learned and best practices regarding evaluations of the cyber vulnerabilities and cyber vulnerability mitigation efforts of major weapon systems across the Department.

''(6) An identification of measures taken to institutionalize evaluations of cyber vulnerabilities of major weapon systems, including an identification of which major weapon systems evaluated under this section will be reevaluated in the future, when these evaluations will occur, and how evaluations will occur for future major weapon systems.

''(7) Information relating to guidance, processes, procedures, or other activities established to mitigate or address the likelihood of cyber vulnerabilities of major weapon systems by incorporation of lessons learned in the research, development, test, evaluation, and acquisition cycle, including promotion of cyber education of the acquisition workforce.

''(8) An identification of systems to be incorporated into or that have been incorporated into the National Security Agency's Strategic Cybersecurity Program and the status of these systems in the Program.

''(9) Any other matters the Secretary determines relevant.

''(h) ESTABLISHING REQUIREMENTS FOR PERIODICITY OF VULNERABILITY REVIEWS.—The Secretary of Defense shall establish policies and requirements for each major weapon system, and the priority critical infrastructure essential to the proper functioning of major weapon systems in broader mission areas, to be re-assessed for cyber vulnerabilities, taking into account upgrades or other modifications to systems and changes in the threat landscape.

''(i) IDENTIFICATION OF SENIOR OFFICIAL.—Each secretary of a military department shall identify a senior official who shall be responsible for ensuring that cyber vulnerability assessments and mitigations for weapon systems and critical infrastructure are planned, funded, and carried out.''

NOTIFICATION OF FOREIGN THREATS TO INFORMATION TECHNOLOGY SYSTEMS IMPACTING NATIONAL SECURITY

Pub. L. 113–291, div. A, title X, § 1078, Dec. 19, 2014, 128 Stat. 3520, provided that:

''(a) NOTIFICATION REQUIRED.—

''(1) IN GENERAL.—Not later than 30 days after the Secretary of Defense determines, through the use of open source information or the use of existing authorities (including section 806 of the National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4260; 10 U.S.C. 2304 note)), that there is evidence of a national security threat described in paragraph (2), the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a notification of such threat.

''(2) NATIONAL SECURITY THREAT.—A national security threat described in this paragraph is a threat to an information technology or telecommunications component or network by an agent of a foreign power in which the compromise of such technology, component, or network poses a significant risk to the programs and operations of the Department of Defense, as determined by the Secretary of Defense.

''(3) FORM.—A notification under this subsection shall be submitted in classified form.

''(b) ACTION PLAN REQUIRED.—In the event that a notification is submitted pursuant to subsection (a), the Secretary shall work with the head of any department or agency affected by the national security threat to develop a plan of action for responding to the concerns leading to the notification.

''(c) AGENT OF A FOREIGN POWER.—In this section, the term 'agent of a foreign power' has the meaning given such term in section 101(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)).''

AUTHORITIES, CAPABILITIES, AND OVERSIGHT OF THE UNITED STATES CYBER COMMAND

Pub. L. 113–66, div. A, title IX, § 932, Dec. 26, 2013, 127 Stat. 829, as amended by Pub. L. 116–283, div. A, title XVII, § 1713(a), Jan. 1, 2021, 134 Stat. 4089; Pub. L. 117–81, div. A, title XV, § 1503(a), Dec. 27, 2021, 135 Stat. 2021; Pub. L. 117–263, div. A, title X, § 1081(d), title XV, § 1501(a), (b)(2)(A), (B), Dec. 23, 2022, 136 Stat. 2797, 2877, 2878, provided that:

''(a) PROVISION OF CERTAIN OPERATIONAL CAPABILITIES.—The Secretary of Defense shall take such actions as the Secretary considers appropriate to provide the United States Cyber Command operational military units with infrastructure and equipment enabling access to the Internet and other types of networks to permit the United States Cyber Command to conduct the peacetime and wartime missions of the Command.

''(b) CYBER RANGES.—

''(1) IN GENERAL.—The Secretary shall review existing cyber ranges and adapt one or more such ranges, as necessary, to support training and exercises of cyber units that are assigned to execute offensive military cyber operations.

''(2) ELEMENTS.—Each range adapted under paragraph (1) shall have the capability to support offensive military operations against targets that—

''(A) have not been previously identified and prepared for attack; and

''(B) must be compromised or neutralized immediately without regard to whether the adversary can detect or attribute the attack.

''[(c) Transferred to section 392a(a) of this title.]

''(d) TRAINING OF CYBER PERSONNEL.—The Secretary shall establish and maintain training capabilities and facilities in the Armed Forces and, as the Secretary considers appropriate, at the United States Cyber Command, to support the needs of the Armed Forces and the United States Cyber Command for personnel who are assigned offensive and defensive cyber missions in the Department of Defense.''

Pub. L. 114–328, div. A, title XVI, § 1643(b), Dec. 23, 2016, 130 Stat. 2602, as amended by Pub. L. 117–263, div. A, title XV, § 1501(c)(3), Dec. 23, 2022, 136 Stat. 2879, provided that: ''The Principal Cyber Advisor to the Secretary of Defense, acting through the cross-functional team under section 392a(a)(3) of title 10, United States Code, and in consultation with the Commander of the United States Cyber Command, shall supervise—

''(1) the development of training standards for computer network operations tool developers for military, civilian, and contractor personnel supporting the cyber mission forces;

''(2) the rapid enhancement of capacity to train personnel to those standards to meet the needs of the cyber mission forces for tool development; and

''(3) actions necessary to ensure timely completion of personnel security investigations and adjudications of security clearances for tool development personnel.''

JOINT FEDERATED CENTERS FOR TRUSTED DEFENSE SYSTEMS FOR THE DEPARTMENT OF DEFENSE

Pub. L. 113–66, div. A, title IX, § 937, Dec. 26, 2013, 127 Stat. 834, as amended by Pub. L. 114–92, div. A, title II, § 231, Nov. 25, 2015, 129 Stat. 778, which provided for the establishment of a joint federation of capabilities to support the trusted defense system needs of the Department of Defense, was repealed by Pub. L. 118–159, div. A, title IX, § 922(c), Dec. 23, 2024, 138 Stat. 2039. See section 4128 of this title.

IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE

Pub. L. 112–239, div. A, title IX, § 933, Jan. 2, 2013, 126 Stat. 1884, as amended by Pub. L. 116–283, div. A, title XVIII, § 1806(e)(2)(A), Jan. 1, 2021, 134 Stat. 4155, provided that:

''(a) BASELINE SOFTWARE ASSURANCE POLICY.—The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Chief Information Officer of the Department of Defense, shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.

''(b) POLICY ELEMENTS.—The baseline software assurance policy under subsection (a) shall—

''(1) require use of appropriate automated vulnerability analysis tools in computer software code during the entire lifecycle of a covered system, including during development, operational testing, operations and sustainment phases, and retirement;

''(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;

''(3) ensure such remediation strategies are translated into contract requirements and evaluated during source selection;

''(4) promote best practices and standards to achieve software security, assurance, and quality; and

''(5) support competition and allow flexibility and compatibility with current or emerging software methodologies.

''(c) VERIFICATION OF EFFECTIVE IMPLEMENTATION.—The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Chief Information Officer of the Department of Defense, shall—

''(1) collect data on implementation of the policy developed under subsection (a) and measure the effectiveness of such policy, including the particular elements required under subsection (b); and

''(2) identify and promote best practices, tools, and standards for developing and validating assured software for the Department of Defense.

''(d) BRIEFING ON ADDITIONAL MEANS OF IMPROVING SOFTWARE ASSURANCE.—Not later than one year after the date of the enactment of this Act [Jan. 2, 2013], the Under Secretary for Acquisition, Technology, and Logistics shall, in coordination with the Chief Information Officer of the Department of Defense, provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the following:

''(1) A research and development strategy to advance capabilities in software assurance and vulnerability detection.

''(2) The state-of-the-art of software assurance analysis and test.

''(3) How the Department might hold contractors liable for software defects or vulnerabilities.

''(e) DEFINITIONS.—In this section:

''(1) COVERED SYSTEM.—The term 'covered system' means any Department of Defense critical information, business, or weapons system that is—

''(A) a major system, as that term is defined in section 3041 of title 10, United States Code;

''(B) a national security system, as that term is defined in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)]; or

''(C) a Department of Defense information system categorized as Mission Assurance Category I in Department of Defense Directive 8500.01E that is funded by the Department of Defense.

''(2) SOFTWARE ASSURANCE.—The term 'software assurance' means the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or

inserted as part of the software, throughout the life cycle.''

REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS

Pub. L. 112–239, div. A, title IX, §941, Jan. 2, 2013, 126 Stat. 1889, which authorized the Secretary of Defense to establish criteria and reporting procedures applicable to penetration of cleared defense contractors' networks or information systems, was transferred to chapter 19 of this title, redesignated as section 393, and amended by Pub. L. 114–92, div. A, title XVI, §1641(a), Nov. 25, 2015, 129 Stat. 1114.

INSIDER THREAT DETECTION

Pub. L. 112–81, div. A, title IX, §922, Dec. 31, 2011, 125 Stat. 1537, as amended by Pub. L. 114–92, div. A, title X, §1073(e), Nov. 25, 2015, 129 Stat. 996, provided that:

''(a) PROGRAM REQUIRED.—The Secretary of Defense shall establish a program for information sharing protection and insider threat mitigation for the information systems of the Department of Defense to detect unauthorized access to, use of, or transmission of classified or controlled unclassified information.

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

''(1) Technology solutions for deployment within the Department of Defense that allow for centralized monitoring and detection of unauthorized activities, including—

''(A) monitoring the use of external ports and read and write capability controls;

''(B) disabling the removable media ports of computers physically or electronically;

''(C) electronic auditing and reporting of unusual and unauthorized user activities;

''(D) using data-loss prevention and data-rights management technology to prevent the unauthorized export of information from a network or to render such information unusable in the event of the unauthorized export of such information;

''(E) a roles-based access certification system;

''(F) cross-domain guards for transfers of information between different networks; and

''(G) patch management for software and security updates.

''(2) Policies and procedures to support such program, including special consideration for policies and procedures related to international and interagency partners and activities in support of ongoing operations in areas of hostilities.

''(3) A governance structure and process that integrates information security and sharing technologies with the policies and procedures referred to in paragraph (2). Such structure and process shall include—

''(A) coordination with the existing security clearance and suitability review process;

''(B) coordination of existing anomaly detection techniques, including those used in counterintelligence investigation or personnel screening activities; and

''(C) updating and expediting of the classification review and marking process.

''(4) A continuing analysis of—

''(A) gaps in security measures under the program; and

''(B) technology, policies, and processes needed to increase the capability of the program beyond the initially established full operating capability to address such gaps.

''(5) A baseline analysis framework that includes measures of performance and effectiveness.

''(6) A plan for how to ensure related security measures are put in place for other departments or agencies with access to Department of Defense networks.

''(7) A plan for enforcement to ensure that the program is being applied and implemented on a uniform and consistent basis.

''(c) OPERATING CAPABILITY.—The Secretary shall ensure the program established under subsection (a)—

''(1) achieves initial operating capability not later than October 1, 2012; and

''(2) achieves full operating capability not later than October 1, 2013.

''(d) REPORT.—Not later than 90 days after the date of the enactment of this Act [Dec. 31, 2011], the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that includes—

''(1) the implementation plan for the program established under subsection (a);

''(2) the resources required to implement the program;

''(3) specific efforts to ensure that implementation does not negatively impact activities in support of ongoing operations in areas of hostilities;

''(4) a definition of the capabilities that will be achieved at initial operating capability and full operating capability, respectively; and

''(5) a description of any other issues related to such implementation that the Secretary considers appropriate.

''(e) BRIEFING REQUIREMENT.—The Secretary shall provide briefings to the Committees on Armed Services of the House of Representatives and the Senate as follows:

''(1) Not later than 90 days after the date of the enactment of this Act [Dec. 31, 2011], a briefing describing the governance structure referred to in subsection (b)(3).

''(2) Not later than 120 days after the date of the enactment of this Act, a briefing detailing the inventory and status of technology solutions deployment referred to in subsection (b)(1), including an identification of the total number of host platforms planned for such deployment, the current number of host platforms that provide appropriate security, and the funding and timeline for remaining deployment.

''(3) Not later than 180 days after the date of the enactment of this Act, a briefing detailing the policies and procedures referred to in subsection (b)(2), including an assessment of the effectiveness of such policies and procedures and an assessment of the potential impact of such policies and procedures on information sharing within the Department of Defense and with interagency and international partners.''

STRATEGY TO ACQUIRE CAPABILITIES TO DETECT PREVIOUSLY UNKNOWN CYBER ATTACKS

Pub. L. 112–81, div. A, title IX, §953, Dec. 31, 2011, 125 Stat. 1550, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall develop and implement a plan to augment the cybersecurity strategy of the Department of Defense through the acquisition of advanced capabilities to discover and isolate penetrations and attacks that were previously unknown and for which signatures have not been developed for incorporation into computer intrusion detection and prevention systems and anti-virus software systems.

''(b) CAPABILITIES.—

''(1) NATURE OF CAPABILITIES.—The capabilities to be acquired under the plan required by subsection (a) shall—

''(A) be adequate to enable well-trained analysts to discover the sophisticated attacks conducted by nation-state adversaries that are categorized as 'advanced persistent threats';

''(B) be appropriate for—

''(i) endpoints or hosts;

''(ii) network-level gateways operated by the Defense Information Systems Agency where the Department of Defense network connects to the public Internet; and

''(iii) global networks owned and operated by private sector Tier 1 Internet Service Providers;

''(C) at the endpoints or hosts, add new discovery capabilities to the Host-Based Security System of the Department, including capabilities such as—

''(i) automatic blocking of unauthorized software programs and accepting approved and vetted programs;

''(ii) constant monitoring of all key computer attributes, settings, and operations (such as registry keys, operations running in memory, security settings, memory tables, event logs, and files); and

''(iii) automatic baselining and remediation of altered computer settings and files;

''(D) at the network-level gateways and internal network peering points, include the sustainment and enhancement of a system that is based on full-packet capture, session reconstruction, extended storage, and advanced analytic tools, by—

''(i) increasing the number and skill level of the analysts assigned to query stored data, whether by contracting for security services, hiring and training Government personnel, or both; and

''(ii) increasing the capacity of the system to handle the rates for data flow through the gateways and the storage requirements specified by the United States Cyber Command; and

''(E) include the behavior-based threat detection capabilities of Tier 1 Internet Service Providers and other companies that operate on the global Internet.

''(2) SOURCE OF CAPABILITIES.—The capabilities to be acquired shall, to the maximum extent practicable, be acquired from commercial sources. In making decisions on the procurement of such capabilities from among competing commercial and Government providers, the Secretary shall take into consideration the needs of other departments and agencies of the Federal Government, State and local governments, and critical infrastructure owned and operated by the private sector for unclassified, affordable, and sustainable commercial solutions.

''(c) INTEGRATION AND MANAGEMENT OF DISCOVERY CAPABILITIES.—The plan required by subsection (a) shall include mechanisms for improving the standardization, organization, and management of the security information and event management systems that are widely deployed across the Department of Defense to improve the ability of United States Cyber Command to understand and control the status and condition of Department networks, including mechanisms to ensure that the security information and event management systems of the Department receive and correlate data collected and analyses conducted at the host or endpoint, at the network gateways, and by Internet Service Providers in order to discover new attacks reliably and rapidly.

''(d) PROVISION FOR CAPABILITY DEMONSTRATIONS.—The plan required by subsection (a) shall provide for the conduct of demonstrations, pilot projects, and other tests on cyber test ranges and operational networks in order to determine and verify that the capabilities to be acquired pursuant to the plan are effective, practical, and affordable.

''(e) REPORT.—Not later than April 1, 2012, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the plan required by subsection (a). The report shall set forth the plan and include a comprehensive description of the actions being undertaken by the Department to implement the plan.''

STRATEGY ON COMPUTER SOFTWARE ASSURANCE

Pub. L. 111–383, div. A, title IX, §932, Jan. 7, 2011, 124 Stat. 4335, as amended by Pub. L. 116–283, div. A, title XVIII, §1806(e)(2)(B), Jan. 1, 2021, 134 Stat. 4155, provided that:

''(a) STRATEGY REQUIRED.—The Secretary of Defense shall develop and implement, by not later than October 1, 2011, a strategy for assuring the security of software and software-based applications for all covered systems.

''(b) COVERED SYSTEMS.—For purposes of this section, a covered system is any critical information system or weapon system of the Department of Defense, including the following:

''(1) A major system, as that term is defined in section 3041 of title 10, United States Code.

''(2) A national security system, as that term is defined in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].

''(3) Any Department of Defense information system categorized as Mission Assurance Category I.

''(4) Any Department of Defense information system categorized as Mission Assurance Category II in accordance with Department of Defense Directive 8500.01E.

''(c) ELEMENTS.—The strategy required by subsection (a) shall include the following:

''(1) Policy and regulations on the following:

''(A) Software assurance generally.

''(B) Contract requirements for software assurance for covered systems in development and production.

''(C) Inclusion of software assurance in milestone reviews and milestone approvals.

''(D) Rigorous test and evaluation of software assurance in development, acceptance, and operational tests.

''(E) Certification and accreditation requirements for software assurance for new systems and for updates for legacy systems, including mechanisms to monitor and enforce reciprocity of certification and accreditation processes among the military departments and Defense Agencies.

''(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

''(2) Allocation of adequate facilities and other resources for test and evaluation and certification and accreditation of software to meet applicable requirements for research and development, systems acquisition, and operations.

''(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber attack by acquiring and improving automated tools for—

''(A) assuring the security of software and software applications during software development;

''(B) detecting vulnerabilities during testing of software; and

''(C) detecting intrusions during real-time monitoring of software applications.

''(4) Mechanisms providing the Department of Defense with the capabilities—

''(A) to monitor systems and applications in order to detect and defeat attempts to penetrate or disable such systems and applications; and

''(B) to ensure that such monitoring capabilities are integrated into the Department of Defense system of cyber defense-in-depth capabilities.

''(5) An update to Committee for National Security Systems Instruction No. 4009, entitled 'National Information Assurance Glossary', to include a standard definition for software security assurance.

''(6) Either—

''(A) mechanisms to ensure that vulnerable Mission Assurance Category III information systems, if penetrated, cannot be used as a foundation for penetration of protected covered systems, and means for assessing the effectiveness of such mechanisms; or

''(B) plans to address critical vulnerabilities in Mission Assurance Category III information systems to prevent their use for intrusions of Mission Assurance Category I systems and Mission Assurance Category II systems.

''(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems.

''(d) REPORT.—Not later than October 1, 2011, the Secretary of Defense shall submit to the congressional de-

fense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the strategy required by subsection (a). The report shall include the following:

''(1) A description of the current status of the strategy required by subsection (a) and of the implementation of the strategy, including a description of the role of the strategy in the risk management by the Department regarding the supply chain and in operational planning for cyber security.

''(2) A description of the risks, if any, that the Department will accept in the strategy due to limitations on funds or other applicable constraints.''

INSTITUTE FOR DEFENSE COMPUTER SECURITY AND INFORMATION PROTECTION

Pub. L. 106–398, §1 [[div. A], title IX, §921], Oct. 30, 2000, 114 Stat. 1654, 1654A–233, provided that:

''(a) ESTABLISHMENT.—The Secretary of Defense shall establish an Institute for Defense Computer Security and Information Protection.

''(b) MISSION.—The Secretary shall require the institute—

''(1) to conduct research and technology development that is relevant to foreseeable computer and network security requirements and information assurance requirements of the Department of Defense with a principal focus on areas not being carried out by other organizations in the private or public sector; and

''(2) to facilitate the exchange of information regarding cyberthreats, technology, tools, and other relevant issues.

''(c) CONTRACTOR OPERATION.—The Secretary shall enter into a contract with a not-for-profit entity, or a consortium of not-for-profit entities, to organize and operate the institute. The Secretary shall use competitive procedures for the selection of the contractor to the extent determined necessary by the Secretary.

''(d) FUNDING.—Of the amount authorized to be appropriated by section 301(5) [114 Stat. 1654A–52], $5,000,000 shall be available for the Institute for Defense Computer Security and Information Protection.

''(e) REPORT.—Not later than April 1, 2001, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the Secretary's plan for implementing this section.''

§ 2224a. Information security: continued applicability of expiring Governmentwide requirements to the Department of Defense

(a) IN GENERAL.—The provisions of subchapter II[1] of chapter 35 of title 44 shall continue to apply through September 30, 2004, with respect to the Department of Defense, notwithstanding the expiration of authority under section 3536[1] of such title.

(b) RESPONSIBILITIES.—In administering the provisions of subchapter II[1] of chapter 35 of title 44 with respect to the Department of Defense after the expiration of authority under section 3536[1] of such title, the Secretary of Defense shall perform the duties set forth in that subchapter for the Director of the Office of Management and Budget.

(Added Pub. L. 107–314, div. A, title X, §1052(b)(1), Dec. 2, 2002, 116 Stat. 2648.)

Editorial Notes

REFERENCES IN TEXT

Provisions relating to the expiration of authority of subchapter II of chapter 35 of title 44, referred to in text, did not appear in section 3536 of title 44 subsequent to the general revision of subchapter II by Pub. L. 107–296, title X, §1001(b)(1), Nov. 25, 2002, 116 Stat. 2259. Subchapter II, as revised by Pub. L. 107–296, was repealed and a new subchapter II enacted by Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3073.

[1] See References in Text note below.

[§ 2225. Repealed. Pub. L. 114–328, div. A, title VIII, §833(b)(2)(A), Dec. 23, 2016, 130 Stat. 2284]

Section, added Pub. L. 106–398, §1 [[div. A], title VIII, §812(a)(1)], Oct. 30, 2000, 114 Stat. 1654, 1654A–212; amended Pub. L. 108–178, §4(b)(2), Dec. 15, 2003, 117 Stat. 2640; Pub. L. 109–364, div. A, title X, §1071(a)(2), Oct. 17, 2006, 120 Stat. 2398; Pub. L. 111–350, §5(b)(6), Jan. 4, 2011, 124 Stat. 3842, related to tracking and management of information technology purchases.

Statutory Notes and Related Subsidiaries

TIME FOR IMPLEMENTATION; APPLICABILITY

Pub. L. 106–398, §1 [[div. A], title VIII, §812(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, which provided that the Secretary of Defense was to collect data as required under section 2225 of this title for all contractual actions covered by such section entered into on or after Oct. 30, 2000, was repealed by Pub. L. 114–328, div. A, title VIII, §833(b)(2)(C)(i), Dec. 23, 2016, 130 Stat. 2284.

GAO REPORT

Pub. L. 106–398, §1 [[div. A], title VIII, §812(c)], Oct. 30, 2000, 114 Stat. 1654, 1654A–214, which directed the Comptroller General to submit to committees of Congress a report on the collection of data under this section not later than 15 months after Oct. 30, 2000, was repealed by Pub. L. 114–328, div. A, title VIII, §833(b)(2)(C)(i), Dec. 23, 2016, 130 Stat. 2284.

[§ 2226. Renumbered § 4602]

[§ 2227. Renumbered § 4601]

§ 2228. Office of Corrosion Policy and Oversight

(a) OFFICE AND DIRECTOR.—(1) There is an Office of Corrosion Policy and Oversight within the Office of the Under Secretary of Defense for Acquisition and Sustainment.

(2) The Office shall be headed by a Director of Corrosion Policy and Oversight, who shall be assigned to such position by the Under Secretary from among civilian employees of the Department of Defense with the qualifications described in paragraph (3). The Director is responsible in the Department of Defense to the Secretary of Defense (after the Under Secretary of Defense for Acquisition and Sustainment) for the prevention and mitigation of corrosion of the military equipment and infrastructure of the Department of Defense.

(3) In order to qualify to be assigned to the position of Director, an individual shall—

(A) have management expertise in, and professional experience with, corrosion project and policy implementation, including an understanding of the effects of corrosion policies on infrastructure; research, development, test, and evaluation; and maintenance; and

(B) have an understanding of Department of Defense budget formulation and execution, policy formulation, and planning and program requirements.

(4) The Secretary of Defense shall designate the position of Director as a critical acquisition position under section 1731 of this title.

(b) DUTIES.—(1) The Director of Corrosion Policy and Oversight (in this section referred to as the ''Director'') shall oversee and coordinate efforts throughout the Department of Defense to prevent and mitigate corrosion of the military equipment and infrastructure of the Department. The duties under this paragraph shall include the duties specified in paragraphs (2) through (5).

(2) The Director shall develop and recommend any policy guidance on the prevention and mitigation of corrosion to be issued by the Secretary of Defense.

(3) The Director shall review the programs and funding levels proposed by the Secretary of each military department during the annual internal Department of Defense budget review process as those programs and funding proposals relate to programs and funding for the prevention and mitigation of corrosion and shall submit to the Secretary of Defense recommendations regarding those programs and proposed funding levels.

(4) The Director shall provide oversight and coordination of the efforts within the Department of Defense to prevent or mitigate corrosion during—

(A) the design, acquisition, and maintenance of military equipment; and

(B) the design, construction, and maintenance of infrastructure.

(5) The Director shall monitor acquisition practices within the Department of Defense—

(A) to ensure that the use of corrosion prevention technologies and the application of corrosion prevention treatments are fully considered during research and development in the acquisition process; and

(B) to ensure that, to the extent determined appropriate for each acquisition program, such technologies and treatments are incorporated into that program, particularly during the engineering and design phases of the acquisition process.

(6) The Director shall ensure that contractors of the Department of Defense carrying out activities for the prevention and mitigation of corrosion of the military equipment and infrastructure of the Department of Defense employ for such activities a substantial number of individuals who have completed, or who are currently enrolled in, a qualified training program.

(c) ADDITIONAL AUTHORITIES FOR DIRECTOR.—The Director is authorized to—

(1) develop, update, and coordinate corrosion training with the Defense Acquisition University;

(2) participate in the process within the Department of Defense for the development of relevant directives and instructions;

(3) interact directly with the corrosion prevention industry, trade associations, other government corrosion prevention agencies, academic research and educational institutions, and scientific organizations engaged in corrosion prevention, including the National Academy of Sciences; and

(4) require that any training or professional development activities for military personnel or civilian employees of the Department of Defense for the prevention and mitigation of corrosion of the military equipment and infrastructure of the Department of Defense are conducted under a qualified training program that trains and certifies individuals in meeting corrosion control standards that are recognized industry-wide.

(d) LONG-TERM STRATEGY.—(1) The Secretary of Defense shall develop and implement a long-term strategy to reduce corrosion and the effects of corrosion on the military equipment and infrastructure of the Department of Defense.

(2) The strategy under paragraph (1) shall include the following:

(A) Expansion of the emphasis on corrosion prevention and mitigation within the Department of Defense to include coverage of infrastructure.

(B) Application uniformly throughout the Department of Defense of requirements and criteria for the testing and certification of new corrosion-prevention technologies for equipment and infrastructure with similar characteristics, similar missions, or similar operating environments.

(C) Implementation of programs, including supporting databases, to ensure that a focused and coordinated approach is taken throughout the Department of Defense to collect, review, validate, and distribute information on proven methods and products that are relevant to the prevention of corrosion of military equipment and infrastructure.

(D) Establishment of a coordinated research and development program for the prevention and mitigation of corrosion for new and existing military equipment and infrastructure that includes a plan to transition new corrosion prevention technologies into operational systems, including through the establishment of memoranda of agreement, joint funding agreements, public-private partnerships, university research and education centers, and other cooperative research agreements.

(3) The strategy shall include, for the matters specified in paragraph (2), the following:

(A) Policy guidance.

(B) Performance measures and milestones.

(C) An assessment of the necessary personnel and funding necessary to accomplish the long-term strategy.

(e) REPORT.—(1) For each budget for a fiscal year, beginning with the budget for fiscal year 2009 and ending with the budget for fiscal year 2022, the Secretary of Defense shall submit, with the defense budget materials, a report on the following:

(A) Funding requirements for the long-term strategy developed under subsection (d).

(B) The estimated composite return on investment achieved by implementing the strategy, and documented in the assessments by the Department of Defense of completed corrosion projects and activities.

(C) For the fiscal year covered by the report and the preceding fiscal year, the funds requested in the budget compared to the funding requirements.

(D) If the full amount of funding requirements is not requested in the budget, the reasons for not including the full amount and a

description of the impact on readiness, logistics, and safety of not fully funding required corrosion prevention and mitigation activities.

(E) For the fiscal year preceding the fiscal year covered by the report, the amount of funds requested in the budget for each project or activity described in subsection (d) compared to the funding requirements for the project or activity.

(F) For the fiscal year preceding the fiscal year covered by the report, a description of the specific amount of funds used for military corrosion projects, the Technical Corrosion Collaboration program, and other corrosion-related activities.

(2)(A) Each report under this section shall include, in an annex to the report, a summary of the most recent report required by subparagraph (B).

(B) Not later than December 31 of each year, through December 31, 2020, the corrosion control and prevention executive of a military department shall submit to the Director of Corrosion Policy and Oversight a report containing recommendations pertaining to the corrosion control and prevention program of the military department. Such report shall include recommendations for the funding levels necessary for the executive to carry out the duties of the executive under this section. The report required under this subparagraph shall—

(i) provide a summary of key accomplishments, goals, and objectives of the corrosion control and prevention program of the military department; and

(ii) include the performance measures used to ensure that the corrosion control and prevention program achieved the goals and objectives described in clause (i).

(f) DEFINITIONS.—In this section:

(1) The term ''corrosion'' means the deterioration of a material or its properties due to a reaction of that material with its chemical environment.

(2) The term ''military equipment'' includes all weapon systems, weapon platforms, vehicles, and munitions of the Department of Defense, and the components of such items.

(3) The term ''infrastructure'' includes all buildings, structures, airfields, port facilities, surface and subterranean utility systems, heating and cooling systems, fuel tanks, pavements, and bridges.

(4) The term ''budget'', with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(5) The term ''defense budget materials'', with respect to a fiscal year, means the materials submitted to Congress by the Secretary of Defense in support of the budget for that fiscal year.

(6) The term ''qualified training program'' means a training program in corrosion control, mitigation, and prevention that is—

(A) offered or accredited by an organization that sets industry corrosion standards; or

(B) an industrial coatings applicator training program registered under the Act of August 16, 1937 (popularly known as the ''National Apprenticeship Act''; 29 U.S.C. 50 et seq.).

(Added Pub. L. 107–314, div. A, title X, §1067(a)(1), Dec. 2, 2002, 116 Stat. 2657; amended Pub. L. 110–181, div. A, title III, §371(a)–(e), Jan. 28, 2008, 122 Stat. 79–81; Pub. L. 110–417, [div. A], title X, §1061(b)(1), Oct. 14, 2008, 122 Stat. 4612; Pub. L. 111–383, div. A, title III, §331, Jan. 7, 2011, 124 Stat. 4185; Pub. L. 112–239, div. A, title III, §341, Jan. 2, 2013, 126 Stat. 1699; Pub. L. 114–328, div. A, title IX, §954(a), (b), Dec. 23, 2016, 130 Stat. 2376, 2377; Pub. L. 115–232, div. A, title VIII, §811(a), Aug. 13, 2018, 132 Stat. 1845; Pub. L. 116–92, div. A, title VIII, §861(j)(13), title XVII, §1731(a)(32), Dec. 20, 2019, 133 Stat. 1520, 1814; Pub. L. 117–81, div. A, title VIII, §813, Dec. 27, 2021, 135 Stat. 1823; Pub. L. 118–31, div. A, title XVIII, §1801(a)(19), Dec. 22, 2023, 137 Stat. 684.)

Editorial Notes

REFERENCES IN TEXT

The Act of August 16, 1937, referred to in subsec. (f)(6)(B), is act Aug. 16, 1937, ch. 663, 50 Stat. 664, popularly known as the National Apprenticeship Act, which is classified generally to chapter 4C (§50 et seq.) of Title 29, Labor. For complete classification of this Act to the Code, see Short Title note set out under section 50 of Title 29 and Tables.

AMENDMENTS

2023—Subsec. (c)(2). Pub. L. 118–31 substituted ''instructions;'' for ''instructions;;''.

2021—Subsec. (b)(6). Pub. L. 117–81, §813(1), added par. (6).

Subsec. (c)(4). Pub. L. 117–81, §813(2), added par. (4).

Subsec. (f)(6). Pub. L. 117–81, §813(3), added par. (6).

2019—Subsec. (a)(2). Pub. L. 116–92, §1731(a)(32), struck out second period at end.

Subsec. (a)(4). Pub. L. 116–92, §861(j)(13), substituted ''under section 1731 of this title'' for ''under section 1733(b)(1)(C) of this title''.

2018—Subsec. (a)(1). Pub. L. 115–232, §811(a)(1), substituted ''and Sustainment'' for '', Technology, and Logistics''.

Subsec. (a)(2). Pub. L. 115–232 substituted ''and Sustainment'' for '', Technology, and Logistics'' and struck out ''The Director shall report directly to the Under Secretary'' after ''infrastructure of the Department of Defense.''

2016—Subsec. (e)(1). Pub. L. 114–328, §954(a)(1), inserted ''and ending with the budget for fiscal year 2022'' after ''2009'' in introductory provisions.

Subsec. (e)(1)(B). Pub. L. 114–328, §954(a)(2), amended subpar. (B) generally. Prior to amendment, subpar. (B) read as follows: ''The return on investment that would be achieved by implementing the strategy, including available validated data on return on investment for completed corrosion projects and activities.''

Subsec. (e)(1)(D). Pub. L. 114–328, §954(a)(3), amended subpar. (D) generally. Prior to amendment, subpar. (D) read as follows: ''An explanation if the funding requirements are not fully funded in the budget.''

Subsec. (e)(1)(F). Pub. L. 114–328, §954(a)(4), struck out ''pilot'' before ''program''.

Subsec. (e)(2). Pub. L. 114–328, §954(b), designated existing provisions as subpar. (A), substituted ''a summary of the most recent report required by subparagraph (B).'' for ''a copy of the annual corrosion report most recently submitted by the corrosion control and prevention executive of each military department under section 903(b)(5) of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417; 122 Stat. 4567; 10 U.S.C. 2228 note).'', and added subpar. (B).

2013—Subsec. (e)(1)(B). Pub. L. 112–239, §341(1)(A), inserted '', including available validated data on return on investment for completed corrosion projects and activities'' before period at end.

Subsec. (e)(1)(E). Pub. L. 112–239, §341(1)(B), substituted ''For the fiscal year preceding the fiscal year covered by the report'' for ''For the fiscal year covered by the report and the preceding fiscal year''.

Subsec. (e)(1)(F). Pub. L. 112–239, §341(1)(C), added subpar. (F).

Subsec. (e)(2), (3). Pub. L. 112–239, §341(2), (3), redesignated par. (3) as (2) and struck out former par. (2) which read as follows: ''Within 60 days after submission of the budget for a fiscal year, the Comptroller General shall provide to the congressional defense committees—

''(A) an analysis of the budget submission for corrosion control and prevention by the Department of Defense; and

''(B) an analysis of the report required under paragraph (1), including the annex to the report described in paragraph (3).''

2011—Subsec. (e)(1)(C). Pub. L. 111–383, §331(1)(A), substituted ''For the fiscal year covered by the report and the preceding fiscal year, the'' for ''The''.

Subsec. (e)(1)(E). Pub. L. 111–383, §331(1)(B), added subpar. (E).

Subsec. (e)(2)(B). Pub. L. 111–383, §331(2), inserted before period at end '', including the annex to the report described in paragraph (3)''.

Subsec. (e)(3). Pub. L. 111–383, §331(3), added par. (3).

2008—Pub. L. 110–181, §371(a)(1), substituted ''Office of Corrosion Policy and Oversight'' for ''Military equipment and infrastructure: prevention and mitigation of corrosion'' in section catchline.

Subsec. (a). Pub. L. 110–181, §371(a)(1), added subsec. (a) and struck out heading and text of former subsec. (a). Former text read as follows: ''The Secretary of Defense shall designate an officer or employee of the Department of Defense, or a standing board or committee of the Department of Defense, as the senior official or organization responsible in the Department to the Secretary of Defense (after the Under Secretary of Defense for Acquisition, Technology, and Logistics) for the prevention and mitigation of corrosion of the military equipment and infrastructure of the Department.''

Subsec. (b)(1). Pub. L. 110–181, §371(a)(2)(A), substituted ''Director of Corrosion Policy and Oversight (in this section referred to as the 'Director')'' for ''official or organization designated under subsection (a)''.

Subsec. (b)(2) to (5). Pub. L. 110–181, §371(a)(2)(B), substituted ''Director'' for ''designated official or organization''.

Subsecs. (c), (d). Pub. L. 110–181, §371(b), added subsec. (c) and redesignated former subsec. (c) as (d). Former subsec. (d) redesignated (f).

Subsec. (d)(2)(D). Pub. L. 110–181, §371(c), as amended by Pub. L. 110–417, inserted '', including through the establishment of memoranda of agreement, joint funding agreements, public-private partnerships, university research and education centers, and other cooperative research agreements'' after ''operational systems''.

Subsec. (e). Pub. L. 110–181, §371(d), added subsec. (e).

Subsec. (f). Pub. L. 110–181, §371(b), redesignated subsec. (d) as (f).

Subsec. (f)(4), (5). Pub. L. 110–181, §371(e), added pars. (4) and (5).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2008 AMENDMENT

Amendment by Pub. L. 110–417 effective Jan. 28, 2008, and as if included in Pub. L. 110–181 as enacted, see section 1061(b) of Pub. L. 110–417, set out as a note under section 6382 of Title 5, Government Organization and Employees.

SUBMISSION OF NOTICE AND PLAN TO CONGRESS BEFORE REORGANIZING, RESTRUCTURING, OR ELIMINATING ANY POSITION OR OFFICE

Pub. L. 115–232, div. A, title VIII, §811(i), Aug. 13, 2018, 132 Stat. 1846, provided that: ''Not less than 30 days before reorganizing, restructuring, or eliminating any position or office specified in this section, the Secretary shall submit to the Committees on Armed Services of the Senate and House of Representatives notice of such reorganization, restructuring, or elimination together with a plan to ensure that mission requirements are met and appropriate oversight is conducted in carrying out such reorganization, restructuring, or elimination. Such plan shall address how user needs will be met and how associated roles and responsibilities will be accomplished for each position or office that the Secretary determines requiring reorganization, restructuring, or elimination.''

IMPLEMENTATION OF CORRECTIVE ACTIONS RESULTING FROM CORROSION STUDY OF THE F–22 AND F–35 AIRCRAFT

Pub. L. 112–81, div. A, title III, §324, Dec. 31, 2011, 125 Stat. 1362, provided that:

''(a) IMPLEMENTATION; CONGRESSIONAL BRIEFING.—Not later than January 31, 2012, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall implement the recommended actions described in subsection (b) and provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the actions taken by the Under Secretary to implement such recommended actions.

''(b) RECOMMENDED ACTIONS.—The recommended actions described in this subsection are the following four recommended actions included in the report of the Government Accountability Office report numbered GAO–11–117R and titled 'Defense Management: DOD Needs to Monitor and Assess Corrective Actions Resulting from Its Corrosion Study of the F–35 Joint Strike Fighter':

''(1) The documentation of program-specific recommendations made as a result of the corrosion study described in subsection (d) with regard to the F–35 and F–22 aircraft and the establishment of a process for monitoring and assessing the effectiveness of the corrective actions taken with respect to such aircraft in response to such recommendations.

''(2) The documentation of program-specific recommendations made as a result of such corrosion study with regard to the other weapon systems identified in the study, specifically the CH–53K helicopter, the Joint High Speed Vessel, the Broad Area Maritime Surveillance Unmanned Aircraft System, and the Joint Light Tactical Vehicle, and the establishment of a process for monitoring and assessing the effectiveness of the corrosion prevention and control programs implemented for such weapons systems in response to such recommendations.

''(3) The documentation of Air Force-specific and Navy-specific recommendations made as a result of such corrosion study and the establishment of a process for monitoring and assessing the effectiveness of the corrective actions taken by the Air Force and the Navy in response to such recommendations.

''(4) The documentation of Department of Defense-wide recommendations made as a result of such corrosion study, the implementation of any needed changes in policies and practices to improve corrosion prevention and control in new systems acquired by the Department, and the establishment of a process for monitoring and assessing the effectiveness of the corrective actions taken by the Department in response to such recommendations.

''(c) DEADLINE FOR COMPLIANCE.—Not later than December 31, 2012, the Under Secretary of Defense for Acquisition, Technology, and Logistics, in conjunction with the directors of the F–35 and F–22 program offices, the directors of the program offices for the weapons systems referred to in subsection (b)(2), the Secretary of the Army, the Secretary of the Air Force, and the Secretary of the Navy, shall—

''(1) take whatever steps necessary to comply with the recommendations documented pursuant to the required implementation under subsection (a) of the recommended actions described in subsection (b); or

''(2) submit to the congressional defense committees written justification of why compliance was not feasible or achieved.

''(d) CORROSION STUDY.—The corrosion study described in this subsection is the study required in House Report 111–166 accompanying H.R. 2647 of the 111th Congress [Pub. L. 111–84] conducted by the Office of the Director of Corrosion Policy and Oversight of the Office of the Secretary of Defense and titled 'Corrosion Evaluation of the F–22 Raptor and F–35 Lightning II Joint Strike Fighter'.''

CORROSION CONTROL AND PREVENTION EXECUTIVES FOR THE MILITARY DEPARTMENTS

Pub. L. 114–328, div. A, title III, §322, Dec. 23, 2016, 130 Stat. 2075, provided that:

''(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2016], the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Director of Corrosion Policy and Oversight for the Department of Defense, shall revise guidance relating to corrosion control and prevention executives to—

''(1) clarify the role of each such executive with respect to assisting the Office of Corrosion Policy and Oversight in holding the appropriate project management office in each military department accountable for submitting the annual report required under [former] section 903(b)(5) of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417; 10 U.S.C. 2228 note [set out below]); and

''(2) ensure that corrosion control and prevention executives emphasize the reduction of corrosion and the effects of corrosion on the military equipment and infrastructure of the Department of Defense, as required in the long-term strategy of the Department of Defense under section 2228(d) of title 10, United States Code.

''(b) CORROSION CONTROL AND PREVENTION EXECUTIVE DEFINED.—In this section, the term 'corrosion control and prevention executive' means the employee of a military department designated as the corrosion control and prevention executive of the department under section 903(a) of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417; 10 U.S.C. 2228 note).''

Pub. L. 110–417, [div. A], title IX, §903, Oct. 14, 2008, 122 Stat. 4566, as amended by Pub. L. 113–66, div. A, title III, §334, title X, §1084(b)(1), Dec. 26, 2013, 127 Stat. 740, 871; Pub. L. 114–328, div. A, title IX, §954(c), Dec. 23, 2016, 130 Stat. 2377; Pub. L. 115–91, div. A, title IX, §924, Dec. 12, 2017, 131 Stat. 1526, provided that:

''(a) REQUIREMENT TO DESIGNATE CORROSION CONTROL AND PREVENTION EXECUTIVE.—Not later than 90 days after the date of the enactment of this Act [Oct. 14, 2008], the Assistant Secretary of each military department with responsibility for acquisition, technology, and logistics shall designate an employee of the military department as the corrosion control and prevention executive. Such executive shall be a senior official in the department with responsibility for coordinating department-level corrosion control and prevention program activities (including budget programming) with the military department and the Office of the Secretary of Defense, the program executive officers of the military departments, and relevant major subordinate commands of the military departments. Each individual so designated shall be a senior civilian employee of the military department concerned in pay grade GS–15 or higher.

''(b) QUALIFICATIONS.—Any individual designated as a corrosion control and prevention executive of a military department pursuant to subsection (a) shall—

''(1) have a working knowledge of corrosion prevention and control;

''(2) have strong program management and communication skills; and

''(3) understand the acquisition, research, development, test, and evaluation, and sustainment policies and procedures of the military department, including for the sustainment of infrastructure.

''(c) DUTIES.—(1) The corrosion control and prevention executive of a military department shall ensure that corrosion control and prevention is maintained in the department's policy and guidance for management of each of the following:

''(A) System acquisition and production, including design and maintenance.

''(B) Research, development, test, and evaluation programs and activities.

''(C) Equipment standardization programs, including international standardization agreements.

''(D) Logistics research and development initiatives.

''(E) Logistics support analysis as it relates to integrated logistic support in the materiel acquisition process.

''(F) Military infrastructure design, construction, and maintenance.

''(2) The corrosion control and prevention executive of a military department shall be responsible for identifying the funding levels necessary to accomplish the items listed in subparagraphs (A) through (F) of paragraph (1).

''(3) The corrosion control and prevention executive of a military department shall, in cooperation with the appropriate staff of the department, develop, support, and provide the rationale for resources—

''(A) to initiate and sustain an effective corrosion control and prevention program in the department;

''(B) to evaluate the program's effectiveness; and

''(C) to ensure that corrosion control and prevention requirements for materiel are reflected in budgeting and policies of the department for the formulation, management, and evaluation of personnel and programs for the entire department, including its reserve components.

''(4) The corrosion control and prevention executive of a military department shall be the principal point of contact of the department to the Director of Corrosion Policy and Oversight (as assigned under section 2228 of title 10, United States Code).

''[(5) Repealed. Pub. L. 114–328, div. A, title IX, §954(c), Dec. 23, 2016, 130 Stat. 2377.]''

DEADLINE FOR DESIGNATION OF RESPONSIBLE OFFICIAL OR ORGANIZATION; INTERIM REPORT; DEADLINE FOR LONG-TERM STRATEGY; GAO REVIEW

Pub. L. 107–314, div. A, title X, §1067(b)–(e), Dec. 2, 2002, 116 Stat. 2658, 2659, directed the Secretary of Defense to designate a responsible official or organization under subsec. (a) of this section not later than 90 days after Dec. 2, 2002, directed the Secretary to submit to Congress a report setting forth the long-term strategy required under subsec. (c) of this section not later than one year after Dec. 2, 2002, and required the Comptroller General to monitor the implementation of such long-term strategy and, not later than 18 months after Dec. 2, 2002, to submit to Congress an assessment of the extent to which that strategy had been implemented.

§ 2229. Strategic policy on prepositioning of materiel and equipment

(a) POLICY REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense shall maintain a strategic policy on the programs of the Department of Defense for prepositioned materiel and equipment. Such policy shall take into account national security threats, strategic mobility, service requirements, support for crisis response elements, and the requirements of the combatant commands, and shall address how the Department's prepositioning programs, both ground and afloat, align with national defense strategies and departmental priorities.

(2) ELEMENTS.—The strategic policy required under paragraph (1) shall include the following elements:

(A) Overarching strategic guidance concerning planning and resource priorities that link the Department of Defense's current and future needs for prepositioned stocks, such as desired responsiveness, to evolving national defense objectives.

(B) A description of the Department's vision for prepositioning programs and the desired end state.

(C) Specific interim goals demonstrating how the vision and end state will be achieved.

(D) A description of the strategic environment, requirements for, and challenges associated with, prepositioning.

(E) Metrics for how the Department will evaluate the extent to which prepositioned assets are achieving defense objectives.

(F) A framework for joint departmental oversight that reviews and synchronizes the military services' prepositioning strategies to minimize potentially duplicative efforts and maximize efficiencies in prepositioned materiel and equipment across the Department of Defense.

(3) JOINT OVERSIGHT.—The Secretary of Defense shall establish joint oversight of the military services' prepositioning efforts to maximize efficiencies across the Department of Defense.

(b) LIMITATION OF DIVERSION OF PREPOSITIONED MATERIEL.—The Secretary of a military department may not divert materiel or equipment from prepositioned stocks except—

(1) in accordance with a change made by the Secretary of Defense to the policy maintained under subsection (a); or

(2) for the purpose of directly supporting a contingency operation or providing humanitarian assistance under chapter 20 of this title.

(c) CONGRESSIONAL NOTIFICATION.—The Secretary of Defense may not implement or change the policy required under subsection (a) until the Secretary submits to the congressional defense committees a report describing the policy or change to the policy.

(d) ANNUAL CERTIFICATION.—(1) Not later than the date of the submission of the President's budget request for a fiscal year under section 1105 of title 31, the Secretary of Defense shall submit to the congressional defense committees a certification in writing that the prepositioned stocks of each of the military departments meet all operations plans, in both fill and readiness, that are in effect as of the date of the submission of the certification.

(2) If, for any year, the Secretary cannot certify that any of the prepositioned stocks meet such operations plans, the Secretary shall include with the certification for that year a list of the operations plans affected, a description of any measures that have been taken to mitigate any risk associated with prepositioned stock shortfalls, and an anticipated timeframe for the replenishment of the stocks.

(3) A certification under this subsection shall be in an unclassified form but may have a classified annex.

(Added Pub. L. 109–364, div. A, title III, § 351(a), Oct. 17, 2006, 120 Stat. 2160; amended Pub. L. 112–81, div. A, title III, § 341(a), Dec. 31, 2011, 125 Stat. 1369; Pub. L. 113–66, div. A, title III, § 321(a), Dec. 26, 2013, 127 Stat. 730; Pub. L. 113–291, div. A, title III, § 322, Dec. 19, 2014, 128 Stat. 3343; Pub. L. 114–92, div. A, title X, § 1081(a)(8), Nov. 25, 2015, 129 Stat. 1001.)

Editorial Notes

AMENDMENTS

2015—Subsec. (d)(1). Pub. L. 114–92 substituted ''a certification in writing'' for ''certification in writing''.

2014—Subsec. (a)(1). Pub. L. 113–291 inserted ''support for crisis response elements,'' after ''service requirements,''.

2013—Subsec. (a). Pub. L. 113–66 amended subsec. (a) generally. Prior to amendment, text read as follows: ''The Secretary of Defense shall maintain a strategic policy on the programs of the Department of Defense for the prepositioning of materiel and equipment. Such policy shall take into account national security threats, strategic mobility, service requirements, and the requirements of the combatant commands.''

2011—Subsec. (d). Pub. L. 112–81 added subsec. (d).

Statutory Notes and Related Subsidiaries

TERMINATION OF REPORTING REQUIREMENTS

For termination, effective Dec. 31, 2021, of provisions in subsec. (d) of this section requiring submittal of annual report to Congress, see section 1061 of Pub. L. 114–328, set out as a note under section 111 of this title.

PLANS REGARDING CONDITION AND MAINTENANCE OF PREPOSITIONED STOCKPILES OF NAVY, MARINE CORPS, AND AIR FORCE

Pub. L. 118–159, div. A, title III, § 333, Dec. 23, 2024, 138 Stat. 1855, provided that:

''(a) PLAN REQUIRED.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2024], the Secretary of the Navy and the Secretary of the Air Force shall each develop a plan to improve the required inspection procedures for the prepositioned stockpiles of the Armed Force concerned, for the purpose of identifying deficiencies and conducting maintenance repairs at levels necessary to ensure such prepositioned stockpiles are mission capable.

''(2) ADDITIONAL REQUIREMENTS FOR NAVY AND MARINE CORPS PLAN.—The plan of the Secretary of the Navy required under paragraph (1) shall include—

''(A) an analysis of the readiness of ships of the Navy and Marine Corps that hold or facilitate the off-loading of prepositioned stockpiles; and

''(B) suggestions for improving inspection procedures of such ships.

''(b) IMPLEMENTATION.—Not later than 30 days after the date on which the Secretary concerned completes the development of a plan under subsection (a), and not less frequently than twice each year thereafter for the three-year period beginning on the date of the enactment of this Act, the Secretary concerned shall inspect the prepositioned stockpiles of the Armed Force concerned in accordance with the procedures under such plan.

''(c) BRIEFINGS.—

''(1) BRIEFING ON PLAN.—Not later than 120 days after the date of the enactment of this Act, each Secretary concerned shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the plan of the Secretary developed under subsection (a).

''(2) BRIEFINGS ON STATUS OF PREPOSITIONED STOCKPILES.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter

for the three-year period beginning on the date of the enactment of this Act, each Secretary concerned shall provide to the congressional defense committees a briefing on the status and condition of the prepositioned stockpiles of the Armed Force concerned.

''(d) DEFINITIONS.—In this section:

''(1) The term 'Armed Force concerned' means—

''(A) the Navy and the Marine Corps, with respect to the Secretary of the Navy;

''(B) the Air Force, with respect to the Secretary of the Air Force.

''(2) The term 'Secretary concerned' means—

''(A) the Secretary of the Navy, with respect to matters concerning the Navy and the Marine Corps; and

''(B) the Secretary of the Air Force, with respect to matters concerning the Air Force.''

PRE-POSITIONED STOCKS OF FINISHED DEFENSE TEXTILE ARTICLES

Pub. L. 118–159, div. A, title III, §336, Dec. 23, 2024, 138 Stat. 1856, provided that:

''(a) IN GENERAL.—The Secretary of Defense may establish pre-positioned stocks of finished defense textile articles, such as uniforms and protective gear, to support the rapid mobilization and sustainment of members of the Armed Forces during a contingency operation.

''(b) PLAN TO REDUCE DELAYS.—The Secretary shall develop a plan for phasing in and targeting policy changes relating to defense textile articles to reduce delinquencies and mitigate delays between policy decisions that may result in the miscalculation of stockpiling in order to ensure ample finished textiles are available to prevent a scenario in which the demand for certain articles is ramping down by the time the supply chain can ramp up to meet the need.''

PLAN REGARDING CONDITION AND MAINTENANCE OF PREPOSITIONED STOCKPILES OF THE ARMY

Pub. L. 118–31, div. A, title III, §349, Dec. 22, 2023, 137 Stat. 228, provided that:

''(a) PLAN REQUIRED.—Not later than 90 days after the date of the enactment of this Act [Dec. 22, 2023], the Secretary of the Army shall develop a plan to improve the required inspection procedures for the prepositioned stockpiles of the Army, for the purpose of identifying deficiencies and conducting maintenance repairs at levels necessary to ensure such prepositioned stockpiles are mission-capable.

''(b) IMPLEMENTATION.—Not later than 30 days after the date on which the Secretary completes the development of the plan under subsection (a), and not less frequently than twice each year thereafter for the three-year period beginning on the date of the enactment of this Act, the Secretary shall inspect the prepositioned stockpiles of the Army in accordance with the procedures under such plan.

''(c) BRIEFINGS.—

''(1) BRIEFING ON PLAN.—Not later than 120 days after the date of the enactment of this Act, the Secretary of the Army shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the plan developed under subsection (a).

''(2) BRIEFINGS ON STATUS OF PREPOSITIONED STOCKPILES.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter for the three-year period beginning on the date of the enactment of this Act, the Secretary of the Army shall provide to the congressional defense committees a briefing on the status and condition of the prepositioned stockpiles of the Army.''

IMPLEMENTATION PLAN AND REPORT

Pub. L. 113–66, div. A, title III, §321(b), (c), Dec. 26, 2013, 127 Stat. 731, 732, as amended by Pub. L. 113–291, div. A, title III, §324, Dec. 19, 2014, 128 Stat. 3343, provided that:

''(b) IMPLEMENTATION PLAN.—

''(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act [Dec. 26, 2013], the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a plan for implementation of the prepositioning strategic policy required under section 2229(a) of title 10, United States Code, as amended by subsection (a).

''(2) ELEMENTS.—The implementation plan required under paragraph (1) shall include the following elements:

''(A) Detailed guidance for how the Department of Defense will achieve the vision, end state, and goals outlined in the strategic policy.

''(B) A comprehensive list of the Department's prepositioned materiel and equipment programs.

''(C) A detailed description of how the plan will be implemented.

''(D) A schedule with milestones for the implementation of the plan.

''(E) An assignment of roles and responsibilities for the implementation of the plan.

''(F) A description of the resources required to implement the plan.

''(G) A description of how the plan will be reviewed and assessed to monitor progress.

''(c) COMPTROLLER GENERAL REPORT.—

''(1) INITIAL REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall review the implementation plan submitted under subsection (b) and the prepositioning strategic policy required under section 2229(a) of title 10, United States Code, as amended by subsection (a), and submit to the congressional defense committees a report describing the findings of such review and including any additional information relating to the propositioning strategic policy and plan that the Comptroller General determines appropriate.

''(2) PROGRESS REPORTS.—Not later than one year after submitting the report required under paragraph (1), and annually thereafter for two years, the Comptroller General shall submit to the congressional defense committees a report assessing the progress of the Department of Defense in implementing its strategic policy and plan for its prepositioned stocks and including any additional information related to the Department's management of its prepositioned stocks that the Comptroller General determines appropriate.''

DEADLINE FOR ESTABLISHMENT OF POLICY

Pub. L. 109–364, div. A, title III, §351(c), Oct. 17, 2006, 120 Stat. 2160, provided that:

''(1) DEADLINE.—Not later than six months after the date of the enactment of this Act [Oct. 17, 2006], the Secretary of Defense shall establish the strategic policy on the programs of the Department of Defense for the prepositioning of materiel and equipment required under section 2229 of title 10, United States Code, as added by subsection (a).

''(2) LIMITATION ON DIVERSION OF PREPOSITIONED MATERIEL.—During the period beginning on the date of the enactment of this Act [Oct. 17, 2006] and ending on the date on which the Secretary of Defense submits the report required under section 2229(c) of title 10, United States Code, on the policy referred to in paragraph (1), the Secretary of a military department may not divert materiel or equipment from prepositioned stocks except for the purpose of directly supporting a contingency operation or providing humanitarian assistance under chapter 20 of that title.''

IMPROVING DEPARTMENT OF DEFENSE SUPPORT FOR CIVIL AUTHORITIES

Pub. L. 109–364, div. A, title III, §359, Oct. 17, 2006, 120 Stat. 2164, provided that:

''(a) CONSULTATION.—In the development of concept plans for the Department of Defense for providing support to civil authorities, the Secretary of Defense may consult with the Secretary of Homeland Security and State governments.

''(b) PREPOSITIONING OF DEPARTMENT OF DEFENSE ASSETS.—The Secretary of Defense may provide for the prepositioning of prepackaged or preidentified basic response assets, such as medical supplies, food and water, and communications equipment, in order to improve the ability of the Department of Defense to rapidly provide support to civil authorities. The prepositioning of basic response assets shall be carried out in a manner consistent with Department of Defense concept plans for providing support to civil authorities and section 2229 of title 10, United States Code, as added by section 351.

''(c) REIMBURSEMENT.—To the extent required by section 1535 of title 31, United States Code, or other applicable law, the Secretary of Defense shall require that the Department of Defense be reimbursed for costs incurred by the Department in the prepositioning of basic response assets under subsection (b).

''(d) MILITARY READINESS.—The Secretary of Defense shall ensure that the prepositioning of basic response assets under subsection (b) does not adversely affect the military preparedness of the United States.

''(e) PROCEDURES AND GUIDELINES.—The Secretary may develop procedures and guidelines applicable to the prepositioning of basic response assets under subsection (b).''

§ 2229a. Annual report on prepositioned materiel and equipment

(a) ANNUAL REPORT REQUIRED.—Not later than the date of the submission of the President's budget request for a fiscal year under section 1105 of title 31, the Secretary of Defense shall submit to the congressional defense committees a report on the status of the materiel in the prepositioned stocks as of the end of the fiscal year preceding the fiscal year during which the report is submitted. Each report shall be unclassified and may contain a classified annex. Each report shall include the following information:

(1) The level of fill for major end items of equipment and spare parts in each prepositioned set as of the end of the fiscal year covered by the report.

(2) The material condition of equipment in the prepositioned stocks as of the end of such fiscal year, grouped by category or major end item.

(3) A list of major end items of equipment drawn from the prepositioned stocks during such fiscal year and a description of how that equipment was used and whether it was returned to the stocks after being used.

(4) A timeline for completely reconstituting any shortfall in the prepositioned stocks.

(5) An estimate of the amount of funds required to completely reconstitute any shortfall in the prepositioned stocks and a description of the Secretary's plan for carrying out such complete reconstitution.

(6) A list of any operations plan affected by any shortfall in the prepositioned stocks and a description of any action taken to mitigate any risk that such a shortfall may create.

(7) A list of any non-standard items slated for inclusion in the prepositioned stocks and a plan for funding the inclusion and sustainment of such items.

(8) A list of any equipment used in support of contingency operations slated for retrograde and subsequent inclusion in the prepositioned stocks.

(9) An efficiency strategy for limited shelf-life medical stock replacement.

(10) The status of efforts to develop a joint strategy, integrate service requirements, and eliminate redundancies.

(11) The operational planning assumptions used in the formulation of prepositioned stock levels and composition.

(12) A list of any strategic plans affected by changes to the levels, composition, or locations of the prepositioned stocks and a description of any action taken to mitigate any risk that such changes may create.

(b) COMPTROLLER GENERAL REVIEW.—(1) The Comptroller General shall review each report submitted under subsection (a) and, as the Comptroller General determines appropriate, submit to the congressional defense committees any additional information that the Comptroller General determines will further inform such committees on issues relating to the status of the materiel in the prepositioned stocks.

(2) The Secretary of Defense shall ensure the full cooperation of the Department of Defense with the Comptroller General for purposes of the conduct of the review required by this subsection, both before and after each report is submitted under subsection (a). The Secretary shall conduct periodic briefings for the Comptroller General on the information covered by each report required under subsection (a) and provide to the Comptroller General access to the data and preliminary results to be used by the Secretary in preparing each such report before the Secretary submits the report to enable the Comptroller General to conduct each review required under paragraph (1) in a timely manner.

(3) The requirement to conduct a review under this subsection shall terminate on September 30, 2015.

(Added Pub. L. 110–181, div. A, title III, § 352(a), Jan. 28, 2008, 122 Stat. 71; amended Pub. L. 112–81, div. A, title III, § 341(b), Dec. 31, 2011, 125 Stat. 1369; Pub. L. 112–239, div. A, title III, § 343, Jan. 2, 2013, 126 Stat. 1700; Pub. L. 114–92, div. A, title III, § 331, Nov. 25, 2015, 129 Stat. 791.)

Editorial Notes

AMENDMENTS

2015—Subsec. (a)(8). Pub. L. 114–92 amended par. (8) generally. Prior to amendment, par. (8) read as follows: ''A list of any equipment used in support of Operation Iraqi Freedom, Operation New Dawn, or Operation Enduring Freedom slated for retrograde and subsequent inclusion in the prepositioned stocks.''

2013—Subsec. (b)(1). Pub. L. 112–239 substituted ''The'' for ''By not later than 120 days after the date on which a report is submitted under subsection (a), the'' and ''each report submitted under subsection (a)'' for ''the report''.

2011—Subsec. (a)(7) to (12). Pub. L. 112–81 added pars. (7) to (12).

Statutory Notes and Related Subsidiaries

TERMINATION OF REPORTING REQUIREMENTS

For termination, effective Dec. 31, 2021, of provisions of this section requiring submittal of annual report to Congress, see section 1061 of Pub. L. 114–328, set out as a note under section 111 of this title.

[§ 2229b. Renumbered § 3072]

CHAPTER 133—FACILITIES FOR RESERVE COMPONENTS

Sec.
2231. Reference to chapter 1803.

Editorial Notes

PRIOR PROVISIONS

A prior chapter 133 was transferred to end of part V of subtitle E of this title and renumbered chapter 1803.

§ 2231. Reference to chapter 1803

Provisions of law relating to facilities for reserve components are set forth in chapter 1803 of this title (beginning with section 18231).

(Added Pub. L. 103–337, div. A, title XVI, § 1664(b)(11), Oct. 5, 1994, 108 Stat. 3011.)

Editorial Notes

PRIOR PROVISIONS

Prior sections 2231 to 2239 were renumbered sections 18231 to 18239 of this title, respectively.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Dec. 1, 1994, except as otherwise provided, see section 1691 of Pub. L. 103–337, set out as a note under section 10001 of this title.

CHAPTER 134—MISCELLANEOUS ADMINISTRATIVE PROVISIONS

Subchapter Sec.
I. Miscellaneous Authorities, Prohibitions, and Limitations on the Use of Appropriated Funds 2241
II. Miscellaneous Administrative Authority 2251

SUBCHAPTER I—MISCELLANEOUS AUTHORITIES, PROHIBITIONS, AND LIMITATIONS ON THE USE OF APPROPRIATED FUNDS

Sec.
2241. Availability of appropriations for certain purposes.
2241a. Prohibition on use of funds for publicity or propaganda purposes within the United States.
2241b. Prohibition on contracts providing payments for activities at sporting events to honor members of the armed forces.
2242. Authority to use appropriated funds for certain investigations and security services.
2243. Authority to use appropriated funds to support student meal programs in overseas defense dependents' schools.
2244. Security investigations.
2244a. Equipment scheduled for retirement or disposal: limitation on expenditures for modifications.
2245. Use of aircraft for proficiency flying: limitation.
[2245a. Repealed.]
2246. Authorization of certain support for military service academy foundations.
[2247 to 2249a. Renumbered or Repealed.]
2249b. Display of State, District of Columbia, commonwealth, and territorial flags by the armed forces.
[2249c to 2249e. Renumbered.]

Editorial Notes

AMENDMENTS

2023—Pub. L. 118–31, div. A, title XVIII, § 1801(a)(20), Dec. 22, 2023, 137 Stat. 684, which directed amendment of the analysis for this chapter by striking item 2249 ''Prohibition on use of funds for documenting economic or employment impact of certain acquisition programs'', was executed to the analysis for this subchapter to reflect the probable intent of Congress.

2022—Pub. L. 117–263, div. A, title V, § 551(b), Dec. 23, 2022, 136 Stat. 2592, added item 2246.

2016—Pub. L. 114–328, div. A, title VIII, § 833(b)(1)(B), title XII, §§ 1241(*o*)(6), 1247(d), Dec. 23, 2016, 130 Stat. 2284, 2512, 2522, struck out items 2245a ''Use of operation and maintenance funds for purchase of investment items: limitation'', 2249a ''Prohibition on providing financial assistance to terrorist countries'', 2249c ''Regional Defense Combating Terrorism Fellowship Program: authority to use appropriated funds for costs associated with education and training of foreign officials'', 2249d ''Distribution to certain foreign personnel of education and training materials and information technology to enhance military interoperability with the armed forces'', and 2249e ''Prohibition on use of funds for assistance to units of foreign security forces that have committed a gross violation of human rights''.

2015—Pub. L. 114–92, div. A, title III, § 341(b), title V, § 573(b)(2), Nov. 25, 2015, 129 Stat. 793, 831, added item 2241b and substituted ''Authority to use appropriated funds to support student meal programs in overseas defense dependents' schools'' for ''Authority to use appropriated funds to support student meal programs in overseas dependents' schools'' in item 2243.

2014—Pub. L. 113–291, div. A, title XII, § 1204(a)(2), Dec. 19, 2014, 128 Stat. 3533, added item 2249e.

2013—Pub. L. 112–239, div. A, title V, § 588(b)(2), Jan. 2, 2013, 126 Stat. 1769, substituted ''Display of State, District of Columbia, commonwealth, and territorial flags by the armed forces.'' for ''Display of State flags: prohibition on use of funds to arbitrarily exclude flag; position and manner of display.'' in item 2249b.

2011—Pub. L. 111–383, div. A, title X, § 1075(b)(30), Jan. 7, 2011, 124 Stat. 4370, transferred item 2241a ''Prohibition on use of funds for publicity or propaganda purposes within the United States'' to appear after item 2241.

2009—Pub. L. 111–84, div. A, title X, § 1031(a)(2), Oct. 28, 2009, 123 Stat. 2448, added item 2241a at the end.

2008—Pub. L. 110–417, [div. A], title XII, § 1205(a)(2), Oct. 14, 2008, 122 Stat. 4624, added item 2249d.

2006—Pub. L. 109–364, div. A, title XII, § 1204(d)(3), Oct. 17, 2006, 120 Stat. 2416, substituted ''Regional Defense Combating Terrorism Fellowship Program: authority to use appropriated funds for costs associated with education and training of foreign officials'' for ''Authority to use appropriated funds for costs of attendance of foreign visitors under Regional Defense Counterterrorism Fellowship Program'' in item 2249c.

Pub. L. 109–163, div. A, title III, §§ 372(b), 373(b), Jan. 6, 2006, 119 Stat. 3210, 3211, added items 2244a and 2245a.

2004—Pub. L. 108–375, div. A, title VI, § 651(f)(3), Oct. 28, 2004, 118 Stat. 1972, struck out items 2246 ''Department of Defense golf courses: limitation on use of appropriated funds'' and 2247 ''Use of appropriated funds for operation of Armed Forces Recreation Center, Europe: limitation''.

2003—Pub. L. 108–136, div. A, title X, § 1045(a)(5)(B), title XII, § 1221(a)(2), Nov. 24, 2003, 117 Stat. 1612, 1651, struck out item 2248 ''Purchase of surety bonds: prohibition'' and added item 2249c.

1996—Pub. L. 104–201, div. A, title X, § 1071(b), Sept. 23, 1996, 110 Stat. 2657, added item 2249b.

Pub. L. 104–106, div. A, title XIII, § 1341(b), div. D, title XLIII, § 4321(b)(2)(B), Feb. 10, 1996, 110 Stat. 485, 672, redesignated item 2247, relating to prohibition on use of funds for documenting economic or employment impact of certain acquisition programs, as 2249 and added item 2249a.