

the Secretary shall expeditiously notify the former member or retired member concerned, or the next of kin of such former member or retired member if such former member or retired member is deceased, of the promotion.

(d) **NATURE OF PROMOTION.**—Any promotion pursuant to this section is honorary, and shall not affect the pay, retired pay, or other benefits from the United States to which the former member or retired member concerned is entitled or would have been entitled based on the military service of such former member or retired member, nor affect any benefits to which any other person is or may become entitled based on the military service of such former member or retired member.

(Added Pub. L. 116-283, div. A, title V, § 523(a), Jan. 1, 2021, 134 Stat. 3597.)

§ 1564. Security clearance investigations

(a) **EXPEDITED PROCESS.**—The Secretary of Defense may prescribe a process for expediting the completion of the background investigations necessary for granting security clearances for—

(1) Department of Defense personnel and Department of Defense contractor personnel who are engaged in sensitive duties that are critical to the national security; and

(2) any individual who—

(A) submits an application for a position as an employee of the Department of Defense for which—

(i) the individual is qualified; and

(ii) a security clearance is required; and

(B) is—

(i) a member of the armed forces who was retired or separated, or is expected to be retired or separated, for physical disability pursuant to chapter 61 of this title;

(ii) the spouse of a member of the armed forces who retires or is separated, after January 7, 2011, for a physical disability as a result of a wound, injuries or illness incurred or aggravated in the line of duty (as determined by the Secretary concerned); or

(iii) the spouse of a member of the armed forces who dies, after January 7, 2011, as a result of a wound, injury, or illness incurred or aggravated in the line of duty (as determined by the Secretary concerned).

(b) **REQUIRED FEATURES.**—The process developed under subsection (a) shall provide for the following:

(1) Quantification of the requirements for background investigations necessary for grants of security clearances for Department of Defense personnel and Department of Defense contractor personnel.

(2) Categorization of personnel on the basis of the degree of sensitivity of their duties and the extent to which those duties are critical to the national security.

(3) Prioritization of the processing of background investigations on the basis of the categories of personnel determined under paragraph (2).

(c) **REINVESTIGATION OR READJUDICATION OF CERTAIN INDIVIDUALS.**—(1) The Secretary of De-

fense shall conduct an investigation or adjudication under subsection (a) of any individual described in paragraph (2) upon—

(A) conviction of that individual by a court of competent jurisdiction for—

(i) sexual assault;

(ii) sexual harassment;

(iii) fraud against the United States; or

(iv) any other violation that the Secretary determines renders that individual susceptible to blackmail or raises serious concern regarding the ability of that individual to hold a security clearance; or

(B) determination by a commanding officer that that individual has committed an offense described in subparagraph (A).

(2) An individual described in this paragraph is an individual who has a security clearance and is—

(A) a flag officer;

(B) a general officer; or

(C) an employee of the Department of Defense in the Senior Executive Service.

(3) The Secretary shall ensure that relevant information on the conviction or determination described in paragraph (1) of an individual described in paragraph (2) during the preceding year, regardless of whether the individual has retired or resigned or has been discharged, released, or otherwise separated from the armed forces, is reported into Federal law enforcement records and security clearance databases, and that such information is transmitted, as appropriate, to other Federal agencies.

(4) In this subsection:

(A) The term “sexual assault” includes rape, sexual assault, forcible sodomy, aggravated sexual contact, abusive sexual contact, and attempts to commit such offenses, as those terms are defined in chapter 47 of this title (the Uniform Code of Military Justice).

(B) The term “sexual harassment” has the meaning given that term in section 1561 of this title.

(C) The term “fraud against the United States” means a violation of section 932 of this title (article 132 of the Uniform Code of Military Justice).

(d) **ANNUAL REVIEW.**—The Secretary shall conduct an annual review of the process prescribed under subsection (a) and shall revise that process as determined necessary in relation to ongoing Department of Defense missions.

(e) **CONSULTATION REQUIREMENT.**—The Secretary shall consult with the Secretaries of the military departments and the heads of Defense Agencies in carrying out this section.

(f) **SENSITIVE DUTIES.**—For the purposes of this section, it is not necessary for the performance of duties to involve classified activities or classified matters in order for the duties to be considered sensitive and critical to the national security.

(g) **USE OF APPROPRIATED FUNDS.**—The Secretary of Defense may use funds authorized to be appropriated to the Department of Defense for operation and maintenance to conduct background investigations under this section for individuals described in subsection (a)(2).

(Added Pub. L. 106-398, §1 [[div. A], title X, §1072(a)], Oct. 30, 2000, 114 Stat. 1654, 1654A-276; amended Pub. L. 111-383, div. A, title III, §351(a), Jan. 7, 2011, 124 Stat. 4192; Pub. L. 112-239, div. A, title X, §1076(e)(1), Jan. 2, 2013, 126 Stat. 1951; Pub. L. 115-232, div. A, title V, §542, Aug. 13, 2018, 132 Stat. 1762; Pub. L. 116-283, div. A, title X, §1081(a)(29), Jan. 1, 2021, 134 Stat. 3872.)

Editorial Notes

AMENDMENTS

2021—Subsec. (c)(2). Pub. L. 116-283 substituted “is an individual” for “in an individual” in introductory provisions.

2018—Subsecs. (c) to (g). Pub. L. 115-232 added subsec. (c) and redesignated former subsecs. (c) to (f) as (d) to (g), respectively.

2013—Subsec. (a)(2)(B)(ii), (iii). Pub. L. 112-239 substituted “January 7, 2011” for “the date of the enactment of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011”.

2011—Subsec. (a). Pub. L. 111-383, §351(a)(1), added subsec. (a) and struck out former subsec. (a). Prior to amendment, text read as follows: “The Secretary of Defense shall prescribe a process for expediting the completion of the background investigations necessary for granting security clearances for Department of Defense personnel and Department of Defense contractor personnel who are engaged in sensitive duties that are critical to the national security.”

Subsec. (f). Pub. L. 111-383, §351(a)(2), added subsec. (f).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2011 AMENDMENT

Pub. L. 111-383, div. A, title III, §351(b), Jan. 7, 2011, 124 Stat. 4193, provided that: “The amendments made by subsection (a) [amending this section] shall apply with respect to a background investigation conducted after the date of the enactment of this Act [Jan. 7, 2011].”

SECURITY CLEARANCE BRIDGE PILOT PROGRAM

Pub. L. 117-263, div. A, title VIII, §882, Dec. 23, 2022, 136 Stat. 2744, provided that:

“(a) IN GENERAL.—The Secretary of Defense, in consultation with the Director of National Intelligence, shall conduct a pilot program to allow the Defense Counterintelligence and Security Agency to sponsor the personal security clearances of the employees of innovative technology companies that are performing a contract of the Department of Defense while the Government completes the adjudication of the facility clearance application of such a [sic] innovative technology company.

“(b) ADDITIONAL REQUIREMENTS.—

“(1) PERSONAL SECURITY CLEARANCE AUTHORITY.—

“(A) IN GENERAL.—Under the pilot program, the Defense Counterintelligence and Security Agency may nominate and sponsor the personal security clearances of the employees of an innovative technology company.

“(B) LIMITATION.—Under the pilot program, the Defense Counterintelligence and Security Agency may sponsor the personal security clearances of employees of not more than 75 innovative technology companies.

“(2) ADJUDICATION OF THE FACILITY CLEARANCE APPLICATION.—Any adjudication of a facility clearance application of an innovative technology company described in subsection (a) shall include an assessment and mitigation of foreign ownership, control, or influence of the innovative technology company, as applicable.

“(c) CLEARANCE TRANSFER.—

“(1) IN GENERAL.—Not later than 30 days after an innovative technology company is granted facility

clearance, the Defense Counterintelligence and Security Agency shall transfer any personal clearances of employees of the innovative technology company held by the Defense Counterintelligence and Security Agency under the pilot program back to the innovative technology company.

“(2) DENIAL OF FACILITY CLEARANCE.—Not later than 10 days after an innovative technology company is denied facility clearance, the Defense Counterintelligence and Security Agency shall release any personal clearances of employees of the innovative technology company held by the Defense Counterintelligence and Security Agency under the pilot program.

“(d) PARTICIPANT SELECTION.—The Under Secretary of Defense for Research and Engineering, in consultation with the Under Secretary of Defense for Acquisition and Sustainment and the service acquisition executive of the military department concerned (as such terms are defined, respectively, in section 101 of title 10, United States Code), shall select innovative technology companies to participate in the pilot program.

“(e) SUNSET.—The pilot program shall terminate on December 31, 2028.

“(f) DEFINITIONS.—In this section:

“(1) FACILITY CLEARANCE.—The term ‘facility clearance’ has the meaning given the term ‘Facility Clearance’ in section 95.5 of title 10, Code of Federal Regulations, or any successor regulation.

“(2) FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE.—The term ‘foreign ownership, control, or influence’ has the meaning given in section 847 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92; 133 Stat. 1505; 10 U.S.C. 4819 note).

“(3) INNOVATIVE TECHNOLOGY COMPANY.—The term ‘innovative technology company’ means a nontraditional defense contractor (as defined in section 3014 of title 10, United States Code) that—

“(A) provides goods or services related to—

“(i) one or more of the 14 critical technology areas described in the memorandum by the Under Secretary of Defense for Research and Engineering issued on February 1, 2022, entitled ‘USD(R&E) Technology Vision for an Era of Competition’; or

“(ii) information technology, software, or hardware that is unavailable from any other entity that possesses a facility clearance; and

“(B) is selected by the Under Secretary of Defense for Research and Engineering under subsection (d) to participate in the pilot program.

“(4) PERSONAL SECURITY CLEARANCE.—The term ‘personal security clearance’ means the security clearance of an individual who has received approval from the Department of Defense to access classified information.

“(5) PILOT PROGRAM.—The term ‘pilot program’ means the pilot program established under subsection (a).”

SECURITY CLEARANCES FOR RECENTLY SEPARATED MEMBERS OF THE ARMED FORCES AND CIVILIAN EMPLOYEES OF THE DEPARTMENT OF DEFENSE

Pub. L. 117-263, div. A, title X, §1045, Dec. 23, 2022, 136 Stat. 2772, provided that:

“(a) IMPROVEMENTS.—

“(1) IN GENERAL.—No later than September 30, 2023, the Secretary of Defense, in coordination with the Director of National Intelligence when acting as the Security Executive Agent, shall establish a process to—

“(A) determine, on the date on which a covered individual separates from the Armed Forces or the Department of Defense (as the case may be), whether the covered individual held an eligibility to access classified information or to occupy a sensitive position immediately prior to such separation and requires an eligibility of an equal or lower level for employment as a covered contractor, except as provided in subsection (b);

“(B) ensure that the re-establishment of trust of a covered individual’s eligibility to occupy a sen-

sitive position takes place expeditiously, in accordance with applicable laws, Executive Orders, or Security Executive Agent policy; and

“(C) ensure that any additional security processing required to re-establish trust to reinstate a covered individual’s eligibility to access classified information or occupy a sensitive position takes place expeditiously.

“(2) COAST GUARD.—In the case of a member of the Armed Forces who is a member of the Coast Guard, the Secretary of Defense shall carry out paragraph (1) in consultation with the Secretary of the Department in which the Coast Guard is operating.

“(b) EXCEPTIONS.—

“(1) IN GENERAL.—Subsection (a) shall not apply with respect to a covered individual—

“(A) whose previously held security clearance is, or was as of the date of separation of the covered individual, under review as a result of one or more potentially disqualifying factors or conditions that have not been fully investigated or mitigated; or

“(B) in the case of a member of the Armed Forces, who separated from the Armed Forces under other than honorable conditions.

“(2) CLARIFICATION OF REVIEW EXCEPTION.—The exception specified in paragraph (1)(A) shall not apply with respect to a routine periodic reinvestigation or a continuous vetting investigation in which no potentially disqualifying factors or conditions have been found.

“(c) DEFINITIONS.—In this section:

“(1) The term ‘covered contractor’ means an individual who is employed by an entity that carries out work under a contract with the Department of Defense or an element of the intelligence community.

“(2) The term ‘covered individual’ means a former member of the Armed Forces or a former civilian employee of the Department of Defense.

“(3) The term ‘intelligence community’ has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).”

DEPARTMENT OF DEFENSE POLICY ON UNCLASSIFIED WORKSPACES AND JOB FUNCTIONS OF PERSONNEL WITH PENDING SECURITY CLEARANCES

Pub. L. 116-283, div. A, title XI, §1101, Jan. 1, 2021, 134 Stat. 3884, provided that:

“(a) POLICY REQUIRED.—The Secretary of Defense shall develop and implement a policy under which a covered individual may occupy a position within the Department of Defense that requires a security clearance to perform appropriate unclassified work, or work commensurate with a security clearance already held by the individual (which may include an interim security clearance), while such individual awaits a final determination with respect to the security clearance required for such position.

“(b) UNCLASSIFIED WORK SPACES.—As part of the policy under subsection (a), the Secretary of Defense shall—

“(1) ensure, to the extent practicable, that all facilities of the Department of Defense at which covered individuals perform job functions have unclassified workspaces; and

“(2) issue guidelines under which appropriately screened individuals, who are not covered individuals, may use the unclassified workspaces on a space-available basis.

“(c) REPORT.—Not later than one year after the date of enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report setting forth the policy required by subsection (a). The report shall include the following:

“(1) Identification of any challenges or impediments to allowing covered individuals fill positions on a probationary basis as described in subsection (a).

“(2) A plan for implementing the policy.

“(3) A description of how existing facilities may be modified to accommodate unclassified workspaces.

“(4) Identification of impediments to making unclassified workspace available.

“(d) COVERED INDIVIDUAL DEFINED.—In this section, the term ‘covered individual’ includes a member of the Armed Forces, a civilian employee of the Department of Defense, or an applicant for a civilian position within the Department of Defense, who has applied for, but who has not yet received, a security clearance that is required for the individual to perform one or more job functions.”

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY ACTIVITIES ON FACILITATING ACCESS TO LOCAL CRIMINAL RECORDS HISTORICAL DATA

Pub. L. 116-92, div. A, title XVI, §1625, Dec. 20, 2019, 133 Stat. 1736, provided that:

“(a) ACTIVITY AUTHORIZED.—Subject to subsection (c), the Director of the Defense Counterintelligence and Security Agency may carry out a set of activities to reduce the time and cost of accessing State, local, and tribal law enforcement records for the background investigations required for current and prospective Federal Government employees and contractors.

“(b) ACTIVITIES CHARACTERIZED.—The activities carried out under subsection (a) shall include only that training, education, and direct assistance to State, local, and tribal communities needed for the purpose of streamlining access to historical criminal record data.

“(c) LIMITATIONS.—

“(1) COMMENCEMENT OF ACTIVITIES.—The Director may not commence carrying out any activities under subsection (a) until the date that is 90 days after the date on which the Director submits the report required by subsection (d)(1).

“(2) LEGAL AND REPORTING OBLIGATIONS.—The Director shall ensure that no activity carried out under subsection (a) obligates a State, local, or tribal entity to any additional legal or reporting obligation to the Defense Counterintelligence and Security Agency.

“(3) SCOPE.—No activity may be carried out under subsection (a) that applies to any matter outside the limited purpose of conducting background investigations for current and prospective Federal Government employees and contractors.

“(4) CONSISTENCY WITH ACCESS PROVIDED.—The Director shall ensure that the activities carried out under subsection (a) are carried out in a manner that is consistent with the access provided by Federal law enforcement entities to the Defense Counterintelligence and Security Agency.

“(d) REPORTS.—

“(1) INITIAL REPORT.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Director shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that details a concept of operation for the set of activities authorized by subsection (a).

“(2) ANNUAL REPORTS.—Not later than one year after the date on which the Director submits a report pursuant to paragraph (1) and not less frequently than once each year thereafter, the Director shall submit to the congressional defense committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a detailed report on the activities carried out by the Director under subsection (a).”

REPORTS ON CONSOLIDATED ADJUDICATION FACILITY OF THE DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Pub. L. 116-92, div. A, title XVI, §1627, Dec. 20, 2019, 133 Stat. 1740, provided that:

“(a) REPORTS.—On a semiannual basis during the period beginning on the date of the enactment of this Act

[Dec. 20, 2019] and ending on the date specified in subsection (b), and annually thereafter, the Director of the Defense Counterintelligence and Security Agency 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 processes in place for adjudicating security clearances and the progress made to address the backlog of security clearance applications, including—

“(1) metrics used by the Director to evaluate the inventory and timeliness of adjudicating security clearance cases; and

“(2) details on the resources used by the Director in carrying out the security clearance mission of the Consolidated Adjudication Facility.

“(b) DETERMINATION AND BRIEFING.—Upon the date on which the Director of the Defense Counterintelligence and Security Agency determines both that the backlog of security clearance adjudications has been substantially eliminated and that the timeline to conduct background investigations reflects the type of investigation being conducted and the level of clearance required, the Director shall—

“(1) notify the congressional defense committees of such determination; and

“(2) provide to such committees a briefing on the progress made by the Director with respect to security clearance adjudications.”

TERMINATION OF REQUIREMENT FOR DEPARTMENT OF DEFENSE FACILITY ACCESS CLEARANCES FOR JOINT VENTURES COMPOSED OF PREVIOUSLY-CLEARED ENTITIES

Pub. L. 116-92, div. A, title XVI, §1629, Dec. 20, 2019, 133 Stat. 1741, provided that: “A clearance for access to a Department of Defense installation or facility may not be required for a joint venture if that joint venture is composed entirely of entities that are currently cleared for access to such installation or facility.”

BACKGROUND AND SECURITY INVESTIGATIONS FOR DEPARTMENT OF DEFENSE PERSONNEL BY DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Pub. L. 115-91, div. A, title IX, §925, Dec. 12, 2017, 131 Stat. 1526, as amended by Pub. L. 115-232, div. A, title IX, §937, Aug. 13, 2018, 132 Stat. 1940, provided that:

“(a) TRANSITION TO DISCHARGE BY DEFENSE SECURITY SERVICE [now DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY].—

“(1) SECRETARIAL AUTHORITY.—The Secretary of Defense has the authority to conduct security, suitability, and credentialing background investigations for Department of Defense personnel. In carrying out such authority, the Secretary may use such authority, or may delegate such authority to another entity.

“(2) PHASED TRANSITION.—As part of providing for the conduct of background investigations initiated by the Department of Defense through the Defense Security Service [now Defense Counterintelligence and Security Agency] by not later than the deadline specified in subsection (b), the Secretary shall, in consultation with the Director of the Office of Personnel Management, provide for a phased transition from the conduct of such investigations by the National Background Investigations Bureau of the Office of Personnel Management to the conduct of such investigations by the Defense Security Service by that deadline.

“(3) TRANSITION ELEMENTS.—The phased transition required by paragraph (2) shall—

“(A) provide for the transition of the conduct of investigations to the Defense Security Service [now Defense Counterintelligence and Security Agency] using a risk management approach; and

“(B) be consistent with the transition from legacy information technology operated by the Office of Personnel Management to the new information technology, including the National Background Investigations System, as described in subsection (f).

“(b) COMMENCEMENT OF IMPLEMENTATION PLAN FOR ONGOING DISCHARGE OF INVESTIGATIONS THROUGH DSS.—Not later than October 1, 2020, the Secretary of Defense shall commence carrying out the implementation plan developed pursuant to section 951(a)(1) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328; 130 Stat. 2371; 10 U.S.C. 1564 note).

“(c) TRANSFER OF CERTAIN FUNCTIONS WITHIN DoD TO DSS.—

“(1) TRANSFER REQUIRED.—For purposes of meeting the requirements in subsections (a) and (b), the Secretary of Defense shall transfer to the Defense Security Service [now Defense Counterintelligence and Security Agency] the functions, personnel, and associated resources of the following organizations:

“(A) The Consolidated Adjudications Facility.

“(B) Other organizations identified by the Secretary for purposes of this paragraph.

“(2) SUPPORTING ORGANIZATIONS.—In addition to the organizations identified pursuant to paragraph (1), the following organizations shall prioritize resources to directly support the execution of requirements in subsections (a) and (b):

“(A) The Office of Cost Analysis and Program Evaluation.

“(B) The Defense Digital Service.

“(C) Other organizations designated by the Secretary for purposes of this paragraph.

“(3) TIMING AND MANNER OF TRANSFER.—The Secretary—

“(A) may carry out the transfer required by paragraph (1) at any time before the date specified in subsection (b) that the Secretary considers appropriate for purposes of this section; and

“(B) shall carry out the transfer in a manner designed to minimize disruptions to the conduct of background investigations for personnel of the Department of Defense.

“(d) TRANSFER OF CERTAIN FUNCTIONS IN OPM TO DSS [now DCSA].—

“(1) IN GENERAL.—For purposes of meeting the requirements in subsections (a) and (b), the Secretary of Defense shall provide for the transfer of the functions described in paragraph (2), and any associated personnel and resources, to the Department of Defense.

“(2) FUNCTIONS.—The functions to be transferred pursuant to paragraph (1) are the following:

“(A) Any personnel security investigations functions transferred by the Secretary to the Director of the Office of Personnel Management pursuant to section 906 of the National Defense Authorization Act for Fiscal Year 2004 (Public Law 108-136; 5 U.S.C. 1101 note).

“(B) Any other functions of the Office of Personnel Management in connection with background investigations initiated by the Department of Defense that the Secretary and the Director jointly consider appropriate.

“(3) ASSESSMENT.—In carrying out the transfer of functions pursuant to paragraph (1), the Secretary shall conduct a comprehensive assessment of workforce requirements for both the Department of Defense and the National Background Investigations Bureau synchronized to the transition plan, including a forecast of workforce needs across the current future-years defense plan for the Department. Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary shall submit to the appropriate congressional committees a report containing the results of the assessment.

“(4) CONSULTATION.—The Secretary shall carry out paragraphs (1), (2), and (3) in consultation with the Director of the Office of Personnel Management and the Director of the Office of Management and Budget.

“(5) LOCATION WITHIN DoD.—Any functions transferred to the Department of Defense pursuant to this subsection shall be located within the Defense Security Service [now Defense Counterintelligence and Security Agency].

“(e) CONDUCT OF CERTAIN ACTIONS.—For purposes of the conduct of background investigations following the commencement of carrying out the implementation plan referred to in subsection (b), the Secretary of Defense shall provide for the following:

“(1) A single capability for the centralized funding, submissions, and processing of all background investigations, from within the Defense Security Service [now Defense Counterintelligence and Security Agency].

“(2) The discharge by the Consolidated Adjudications Facility, from within the Defense Security Service [now Defense Counterintelligence and Security Agency] pursuant to transfer under subsection (c), of adjudications in connection with the following:

“(A) Background investigations.

“(B) Continuous evaluation and vetting checks.

“(f) ENHANCEMENT OF INFORMATION TECHNOLOGY CAPABILITIES OF NBIS.—

“(1) IN GENERAL.—The Secretary of Defense shall conduct a review of the information technology capabilities of the National Background Investigations System in order to determine whether enhancements to such capabilities are required for the following:

“(A) Support for background investigations pursuant to this section and section 951 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328; 130 Stat. 2371; 10 U.S.C. 1564 note).

“(B) Support of the National Background Investigations Bureau.

“(C) Execution of the conduct of background investigations initiated by the Department of Defense pursuant to this section, including submissions and adjudications.

“(2) COMMON COMPONENT.—In providing for the transition and operation of the National Background Investigations System as described in paragraph (1)(C), the Secretary shall develop a common component of the System usable for background investigations by both the Defense Security Service [now Defense Counterintelligence and Security Agency] and the National Background Investigations Bureau.

“(3) ENHANCEMENTS.—If the review pursuant to paragraph (1) determines that enhancements described in that paragraph are required, the Secretary shall carry out such enhancements.

“(4) CONSULTATION.—The Secretary shall carry out this subsection in consultation with the Director of the Office of Personnel Management.

“(g) USE OF CERTAIN PRIVATE INDUSTRY DATA.—In carrying out background and security investigations pursuant to this section and section 951 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328; 130 Stat. 2371; 10 U.S.C. 1564 note), the Secretary of Defense may use background materials collected on individuals by the private sector, in accordance with national policies and standards, that are applicable to such investigations, including materials as follows:

“(1) Financial information, including credit scores and credit status.

“(2) Criminal records.

“(3) Drug screening.

“(4) Verifications of information on resumes and employment applications, such as previous employers, educational achievement, and educational institutions attended.

“(5) Other publicly available electronic information.

“(h) SECURITY CLEARANCES FOR CONTRACTOR PERSONNEL.—

“(1) IN GENERAL.—The Secretary of Defense shall review the requirements of the Department of Defense relating to position sensitivity designations for contractor personnel in order to determine whether such requirements may be reassessed or modified to reduce the number and range of contractor personnel who are issued security clearances in connection with work under contracts with the Department.

“(2) GUIDANCE.—The Secretary shall issue guidance to program managers, contracting officers, and security personnel of the Department specifying requirements for the review of contractor position sensitivity designations and the number of contractor personnel of the Department who are issued security clearances for the purposes of determining whether the number of such personnel who are issued security clearances should and can be reduced.

“(i) PERSONNEL TO SUPPORT THE TRANSFER OF FUNCTIONS.—The Secretary of Defense shall authorize the Director of the Defense Security Service [now Defense Counterintelligence and Security Agency] to promptly increase the number of personnel of the Defense Security Service for the purpose of beginning the establishment and expansion of investigative capacity to support the phased transfer of investigative functions from the Office of Personnel Management to the Department of Defense under this section. The Director of Cost Analysis and Program Assessment shall advise the Secretary on the size of the initial investigative workforce and the rate of growth of that workforce.

“(j) REPORT ON FUTURE PERIODIC REINVESTIGATIONS, INSIDER THREAT, AND CONTINUOUS VETTING.—

“(1) REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall submit to the appropriate congressional committees a report that includes the following:

“(A) An assessment of the feasibility and advisability of periodic reinvestigations of backgrounds of Government and contractor personnel with security clearances, including lessons from all of the continuous evaluation pilots being conducted throughout the Government, and identification of new or additional data sources and data analytic tools needed for improving current continuous evaluation or vetting capabilities.

“(B) A plan to provide the Government with an enhanced risk management model that reduces the gaps in coverage perpetuated by the current time-based periodic reinvestigations model, particularly in light of the increasing use of continuous background evaluations of personnel referred to in subparagraph (A).

“(C) A plan for expanding continuous background vetting capabilities, such as the Installation Matching Engine for Security and Analysis, to the broader population, including those at the lowest tiers and levels of access, which plan shall include details to ensure that all individuals credentialed for physical access to Department of Defense facilities and installations are vetted to the same level of fitness determinations and subject to appropriate continuous vetting.

“(D) A plan to fully integrate and incorporate insider threat data, tools, and capabilities into the new end-to-end vetting processes and supporting information technology established by the Defense Security Service [now Defense Counterintelligence and Security Agency] to ensure a holistic and transformational approach to detecting, deterring, and mitigating threats posed by trusted insiders.

“(2) CONSULTATION.—The Secretary shall prepare the report under paragraph (1) in consultation with the Director of National Intelligence and the Director of the Office of Personnel Management.

“(k) QUARTERLY AND ANNUAL BRIEFINGS AND REPORTS.—

“(1) ANNUAL ASSESSMENT OF TIMELINESS.—Not later than December 31, 2018, and each December 31 thereafter through the date specified in paragraph (4), the Security Executive Agent, in coordination with the Chair and other Principals of the Security, Suitability, and Credentialing Performance Accountability Council, shall submit to the appropriate committees of Congress a report on the timeliness of personnel security clearance initiations, investigations, and adjudications, by clearance level, for both initial investigations and periodic reinvestigations during

the prior fiscal year for Government and contractor employees, including the following:

“(A) The average periods of time taken by each authorized investigative agency and authorized adjudicative agency to initiate cases, conduct investigations, and adjudicate cases as compared with established timeliness objectives, from the date a completed security clearance application is received to the date of adjudication and notification to the subject and the subject’s employer.

“(B) The number of initial investigations and periodic reinvestigations initiated and adjudicated by each authorized adjudicative agency.

“(C) The number of initial investigations and periodic reinvestigations carried over from prior fiscal years by each authorized investigative and adjudicative agency.

“(D) The number of initial investigations and periodic reinvestigations that resulted in a denial or revocation of a security clearance by each authorized adjudicative agency.

“(E) The costs to the executive branch related to personnel security clearance initiations, investigations, adjudications, revocations, and continuous evaluation.

“(F) A discussion of any impediments to the timely processing of personnel security clearances.

“(G) The number of clearance holders enrolled in continuous evaluation and the numbers and types of adverse actions taken as a result by each authorized adjudicative agency.

“(H) The number of personnel security clearance cases, both initial investigations and periodic reinvestigations, awaiting or under investigation by the National Background Investigations Bureau.

“(I) Other information as appropriate, including any recommendations to improve the timeliness and efficiency of personnel security clearance initiations, investigations, and adjudications.

“(2) QUARTERLY BRIEFINGS.—Not later than the end of each calendar-year quarter beginning after January 1, 2018, through the date specified in paragraph (4), the Secretary of Defense shall provide the appropriate congressional committees a briefing on the progress of the Secretary in carrying out the requirements of this section during that calendar-year quarter. Until the backlog of security clearance applications at the National Background Investigations Bureau is eliminated, each quarterly briefing shall also include the current status of the backlog and the resulting mission and resource impact to the Department of Defense and the defense industrial base. Until the phased transition described in subsection (a) is complete, each quarterly briefing shall also include identification of any resources planned for movement from the National Background Investigations Bureau to the Department of Defense during the next calendar-year quarter.

“(3) ANNUAL REPORTS.—Not later than December 31, 2018, and each December 31 thereafter through the date specified in paragraph (4), the Secretary of Defense shall submit to the appropriate congressional committees a report on the following for the calendar year in which the report is to be submitted:

“(A) The status of the Secretary in meeting the requirements in subsections (a), (b), and (c).

“(B) The status of any transfers to be carried out pursuant to subsection (d).

“(C) An assessment of the personnel security capabilities of the Department of Defense.

“(D) The average periods of time taken by each authorized investigative agency and authorized adjudicative agency to initiate cases, conduct investigations, and adjudicate cases as compared with established timeliness objectives, from the date a completed security clearance application is received to the date of adjudication and notification to the subject and the subject’s employer.

“(E) The number of initial investigations and periodic reinvestigations initiated and adjudicated by each authorized adjudicative agency.

“(F) The number of initial investigations and periodic reinvestigations carried over from prior fiscal years by each authorized investigative and adjudicative agency.

“(G) The number of initial investigations and periodic reinvestigations that resulted in a denial or revocation of a security clearance by each authorized adjudicative agency.

“(H) The number of denials or revocations of a security clearance by each authorized adjudicative agency that occurred separately from a periodic reinvestigation.

“(I) The costs to the Department of Defense related to personnel security clearance initiations, investigations, adjudications, revocations, and continuous evaluation.

“(J) A discussion of any impediments to the timely processing of personnel security clearances.

“(K) The number of clearance holders enrolled in continuous evaluation and the numbers and types of adverse actions taken as a result.

“(L) The number of personnel security clearance cases, both initial investigations and periodic reinvestigations, awaiting or under investigation by the National Background Investigations Bureau.

“(M) Other information that the Secretary considers appropriate, including any recommendations to improve the timeliness and efficiency of personnel security clearance initiations, investigations, and adjudications.

“(4) TERMINATION.—No briefing or report is required under this subsection after December 31, 2021.

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

“(1) the Committees on Armed Services, Appropriations, Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

“(2) the Committees on Armed Services, Appropriations, Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives.”

ENHANCED SECURITY PROGRAMS FOR DEPARTMENT OF DEFENSE PERSONNEL AND INNOVATION INITIATIVES

Pub. L. 114-328, div. A, title IX, §951, Dec. 23, 2016, 130 Stat. 2371, provided that:

“(a) ENHANCEMENT OF SECURITY PROGRAMS GENERALLY.—

“(1) PERSONNEL BACKGROUND AND SECURITY PLAN REQUIRED.—The Secretary of Defense shall develop an implementation plan for the Defense Security Service [now Defense Counterintelligence and Security Agency] to conduct, after October 1, 2017, background investigations for personnel of the Department of Defense whose investigations are adjudicated by the Consolidated Adjudication Facility of the Department. The Secretary shall submit the implementation plan to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] by not later than August 1, 2017.

“(2) PLAN FOR POTENTIAL TRANSFER OF INVESTIGATIVE PERSONNEL TO DEPARTMENT OF DEFENSE.—Not later than October 1, 2017, the Secretary and the Director of the Office of Personnel Management shall develop a plan to transfer Government investigative personnel and contracted resources to the Department in proportion to the background and security investigative workload that would be assumed by the Department if the plan required by paragraph (1) were implemented.

“(3) REPORT.—Not later than August 1, 2017, the Secretary shall submit to the congressional defense committees a report on the number of full-time equivalent employees of the management headquarters of the Department that would be required by the Defense Security Service [now Defense Counterintelligence and Security Agency] to carry out the plan developed under paragraph (1).

“(4) COLLECTION, STORAGE, AND RETENTION OF INFORMATION BY INSIDER THREAT PROGRAMS.—In order to enable detection and mitigation of potential insider threats, the Secretary shall ensure that insider threat programs of the Department collect, store, and retain information from the following:

- “(A) Personnel security.
- “(B) Physical security.
- “(C) Information security.
- “(D) Law enforcement.
- “(E) Counterintelligence.
- “(F) User activity monitoring.
- “(G) Information assurance.
- “(H) Such other data sources as the Secretary considers necessary and appropriate.

“(b) ELEMENTS OF SYSTEM.—

“(1) IN GENERAL.—In developing a system for the performance of background investigations for personnel in carrying out subsection (a), the Secretary shall—

- “(A) conduct a review of security clearance business processes and, to the extent practicable, modify such processes to maximize compatibility with the security clearance information technology architecture to minimize the need for customization of the system;
- “(B) conduct business process mapping of the business processes described in subparagraph (A);
- “(C) use spiral development and incremental acquisition practices to rapidly deploy the system, including through the use of prototyping and open architecture principles;
- “(D) establish a process to identify and limit interfaces with legacy systems and to limit customization of any commercial information technology tools used;
- “(E) establish automated processes for measuring the performance goals of the system;
- “(F) incorporate capabilities for the continuous monitoring of network security and the mitigation of insider threats to the system;
- “(G) institute a program to collect and maintain data and metrics on the background investigation process; and
- “(H) establish a council (to be known as the ‘Department of Defense Background Investigations Rate Council’) to advise and advocate for rate efficiencies for background clearance investigation rates, and to negotiate rates for background investigation services provided to outsiders [sic] entities and agencies when requested.

“(2) COMPLETION DATE.—The Secretary shall complete the development and implementation of the system described in paragraph (1) by not later than September 30, 2019.

“(c) ESTABLISHMENT OF ENHANCED SECURITY PROGRAM TO SUPPORT DEPARTMENT OF DEFENSE INNOVATION INITIATIVE.—

“(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary shall establish a personnel security program, and take such other actions as the Secretary considers appropriate, to support the Innovation Initiative of the Department to better leverage commercial technology.

“(2) POLICIES AND PROCEDURES.—In establishing the program required by paragraph (1), the Secretary shall develop policies and procedures to rapidly and inexpensively investigate and adjudicate security clearances for personnel from commercial companies with innovative technologies and solutions to enable such companies to receive relevant threat reporting and to propose solutions for a broader set of Department requirements.

“(3) ACCESS TO CLASSIFIED INFORMATION.—The Secretary shall ensure that access to classified information under the program required by paragraph (1) is not contingent on a company already being under contract with the Department.

“(4) AWARD OF SECURITY CLEARANCES.—The Secretary may award secret clearances under the pro-

gram required by paragraph (1) for limited purposes and periods relating to the acquisition or modification of capabilities and services.

“(d) UPDATED GUIDANCE AND REVIEW OF POLICIES.—

“(1) REVIEW OF APPLICABLE LAWS.—The Secretary shall review laws, regulations, and executive orders relating to the maintenance of personnel security clearance information by the Federal Government, including the investigation timeline metrics established in the Intelligence Reform and Prevention of Terrorism Act of 2004 (Public Law 108-458 [see Tables for classification]). The review should also identify recommendations to eliminate duplicative or outdated authorities in current executive orders, regulations and guidance. Not later than 90 days after the date of the enactment of this Act [Dec. 23, 2016], the Secretary shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing that includes—

- “(A) the results of the review; and
- “(B) recommendations, if any, for consolidating and clarifying laws, regulations, and executive orders relating to the maintenance of personnel security clearance information by the Federal Government.

“(2) RECIPROCITY DIRECTIVE.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall coordinate with the Security Executive Agent, in consultation with the Suitability Executive Agent, to issue an updated reciprocity directive that accounts for security policy changes associated with new position designation regulations under section 1400 of title 5, Code of Federal Regulations, new continuous evaluation policies, and new Federal investigative standards.

“(3) IMPLEMENTATION DIRECTIVES.—The Secretary, working with the Security Executive Agent and the Suitability Executive Agent, shall jointly develop and issue directives on—

- “(A) completing the implementation of the National Security Sensitive Position designations required by section 1400 of title 5, Code of Federal Regulations; and
- “(B) aligning to the maximum practical extent the investigative and adjudicative standards and criteria for positions requiring access to classified information and national security sensitive positions not requiring access to classified information to ensure effective and efficient reciprocity and consistent designation of like-positions across the Federal Government.

“(e) WAIVER OF CERTAIN DEADLINES.—For each of fiscal years 2017 through 2019, the Secretary may waive any background investigation timeline specified in the Intelligence Reform and Prevention of Terrorism Act of 2004 if the Secretary submits to the appropriate committees of Congress a written notification on the waiver not later than 30 days before the beginning of the fiscal year concerned.

“(f) DEFINITIONS.—In this section:

“(1) The term ‘appropriate committees of Congress’ has the meaning given that term in section 3001(a)(8) of the Intelligence Reform and Prevention of Terrorism Act of 2004 (50 U.S.C. 3341(a)(8)).

“(2) The term ‘business process mapping’ has the meaning given that term in section 2222(i) of title 10, United States Code.

“(3) The term ‘insider threat’ means, with respect to the Department, a threat presented by a person who—

- “(A) has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department; and
- “(B) wittingly, or unwittingly, commits—

- “(i) an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or

“(ii) a destructive act, which may include physical harm to another in the workplace.”

REFORM AND IMPROVEMENT OF PERSONNEL SECURITY, INSIDER THREAT DETECTION AND PREVENTION, AND PHYSICAL SECURITY

Pub. L. 114-92, div. A, title X, §1086, Nov. 25, 2015, 129 Stat. 1006, as amended by Pub. L. 114-328, div. A, title X, §1081(c)(7), Dec. 23, 2016, 130 Stat. 2420, provided that:

“(a) PERSONNEL SECURITY AND INSIDER THREAT PROTECTION IN DEPARTMENT OF DEFENSE.—

“(1) PLANS AND SCHEDULES.—Consistent with the Memorandum of the Secretary of Defense dated March 18, 2014, regarding the recommendations of the reviews of the Washington Navy Yard shooting, the Secretary of Defense shall develop plans and schedules—

“(A) to implement a continuous evaluation capability for the national security population for which clearance adjudications are conducted by the Department of Defense Central Adjudication Facility, in coordination with the heads of other relevant agencies;

“(B) to produce a Department-wide insider threat strategy and implementation plan, which includes—

“(i) resourcing for the Defense Insider Threat Management and Analysis Center and component insider threat programs, and

“(ii) alignment of insider threat protection programs with continuous evaluation capabilities and processes for personnel security;

“(C) to centralize the authority, accountability, and programmatic integration responsibilities, including fiscal control, for personnel security and insider threat protection under the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security];

“(D) to develop a defense security enterprise reform investment strategy to ensure a consistent, long-term focus on funding to strengthen all of the Department’s security and insider threat programs, policies, functions, and information technology capabilities, including detecting threat behaviors conveyed in the cyber domain, in a manner that keeps pace with evolving threats and risks;

“(E) to resource and expedite deployment of the Identity Management Enterprise Services Architecture; and

“(F) to implement the recommendations contained in the study conducted by the Director of Cost Analysis and Program Evaluation required by section 907 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66; 10 U.S.C. 1564 note), including, specifically, the recommendations to centrally manage and regulate Department of Defense requests for personnel security background investigations.

“(2) REPORTING REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act [Nov. 25, 2015], the Secretary of Defense shall submit to the appropriate committees of Congress a report describing the plans and schedules required under paragraph (1).

“(b) PHYSICAL AND LOGICAL ACCESS.—Not later than 270 days after the date of the enactment of this Act—

“(1) the Secretary of Defense shall define physical and logical access standards, capabilities, and processes applicable to all personnel with access to Department of Defense installations and information technology systems, including—

“(A) periodic or regularized background or records checks appropriate to the type of physical or logical access involved, the security level, the category of individuals authorized, and the level of access to be granted;

“(B) standards and methods for verifying the identity of individuals seeking access; and

“(C) electronic attribute-based access controls that are appropriate for the type of access and facility or information technology system involved;

“(2) the Director of the Office of Management and Budget and the Chair of the Performance Accountability Council, in coordination with the Secretary of Defense, the Administrator of General Services, and, when appropriate, the Director of National Intelligence, and in consultation with representatives from stakeholder organizations, shall design a capability to share and apply electronic identity information across the Government to enable real-time, risk-managed physical and logical access decisions; and

“(3) the Director of the Office of Management and Budget, in conjunction with the Director of the Office of Personnel Management and in consultation with representatives from stakeholder organizations, shall establish investigative and adjudicative standards for the periodic or regularized reevaluation of the eligibility of an individual to retain credentials issued pursuant to Homeland Security Presidential Directive 12 (dated August 27, 2004), as appropriate, but not less frequently than the authorization period of the issued credentials.

“(c) SECURITY ENTERPRISE MANAGEMENT.—Not later than 180 days after the date of enactment of this Act [Nov. 25, 2015], the Director of the Office of Management and Budget shall—

“(1) formalize the Security, Suitability, and Credentialing Line of Business; and

“(2) submit to the appropriate congressional committee a report that describes plans—

“(A) for oversight by the Office of Management and Budget of activities of the executive branch of the Government for personnel security, suitability, and credentialing;

“(B) to designate enterprise shared services to optimize investments;

“(C) to define and implement data standards to support common electronic access to critical Government records; and

“(D) to reduce the burden placed on Government data providers by centralizing requests for records access and ensuring proper sharing of the data with appropriate investigative and adjudicative elements.

“(d) RECIPROCITY MANAGEMENT.—Not later than two years after the date of the enactment of this Act, the Chair of the Performance Accountability Council shall ensure that—

“(1) a centralized system is available to serve as the reciprocity management system for the Federal Government; and

“(2) the centralized system described in paragraph (1) is aligned with, and incorporates results from, continuous evaluation and other enterprise reform initiatives.

“(e) REPORTING REQUIREMENTS IMPLEMENTATION.—Not later than 180 days after the date of enactment of this Act, the Chair of the Performance Accountability Council, in coordination with the Security Executive Agent, the Suitability Executive Agent, and the Secretary of Defense, shall jointly develop a plan to—

“(1) implement the Security Executive Agent Directive on common, standardized employee and contractor security reporting requirements;

“(2) establish and implement uniform reporting requirements for employees and Federal contractors, according to risk, relative to the safety of the workforce and protection of the most sensitive information of the Government; and

“(3) ensure that reported information is shared appropriately.

“(f) Access to Criminal History Records for National Security and Other Purposes.—

“(1) DEFINITION.—[Amended section 9101 of Title 5, Government Organization and Employees.]

“(2) COVERED AGENCIES.—[Amended section 9101 of Title 5.]

“(3) APPLICABLE PURPOSES OF INVESTIGATIONS.—[Amended section 9101 of Title 5.]

“(4) BIOMETRIC AND BIOGRAPHIC SEARCHES.—[Amended section 9101 of Title 5.]

“(5) USE OF MOST COST-EFFECTIVE SYSTEM.—[Amended section 9101 of Title 5.]

“(6) SEALED OR EXPUNGED RECORDS; JUVENILE RECORDS.—

“(A) IN GENERAL.—[Amended section 9101 of Title 5.]

“(B) REGULATIONS.—

“(i) DEFINITION.—In this subparagraph, the terms ‘Security Executive Agent’ and ‘Suitability Executive Agent’ mean the Security Executive Agent and the Suitability Executive Agent, respectively, established under Executive Order 13467 (73 Fed. Reg. 38103) [50 U.S.C. 3161 note], or any successor thereto.

“(ii) DEVELOPMENT; PROMULGATION.—The Security Executive Agent shall—

“(I) not later than 45 days after the date of enactment of this Act [Nov. 25, 2015], and in conjunction with the Suitability Executive Agent and the Attorney General, begin developing regulations to implement the amendments made by subparagraph (A); and

“(II) not later than 120 days after the date of enactment of this Act, promulgate regulations to implement the amendments made by subparagraph (A).

“(C) SENSE OF CONGRESS.—It is the sense of Congress that the Federal Government should not uniformly reject applicants for employment with the Federal Government or Federal contractors based on—

“(i) sealed or expunged criminal records; or

“(ii) juvenile records.

“(7) INTERACTION WITH LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ABROAD.—[Amended section 9101 of Title 5.]

“(8) CLARIFICATION OF SECURITY REQUIREMENTS FOR CONTRACTORS CONDUCTING BACKGROUND INVESTIGATIONS.—[Amended section 9101 of Title 5.]

“(9) CLARIFICATION REGARDING ADVERSE ACTIONS.—[Amended section 7512 of Title 5.]

“(10) ANNUAL REPORT BY SUITABILITY AND SECURITY CLEARANCE PERFORMANCE ACCOUNTABILITY COUNCIL.—[Amended section 9101 of Title 5.]

“(11) GAO REPORT ON ENHANCING INTEROPERABILITY AND REDUCING REDUNDANCY IN FEDERAL CRITICAL INFRASTRUCTURE PROTECTION ACCESS CONTROL, BACKGROUND CHECK, AND CREDENTIALING STANDARDS.—

“(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives], the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the background check, access control, and credentialing requirements of Federal programs for the protection of critical infrastructure and key resources.

“(B) CONTENTS.—The Comptroller General shall include in the report required under subparagraph (A)—

“(i) a summary of the major characteristics of each such Federal program, including the types of infrastructure and resources covered;

“(ii) a comparison of the requirements, whether mandatory or voluntary in nature, for regulated entities under each such program to—

“(I) conduct background checks on employees, contractors, and other individuals;

“(II) adjudicate the results of a background check, including the utilization of a standardized set of disqualifying offenses or the consideration of minor, non-violent, or juvenile offenses; and

“(III) establish access control systems to deter unauthorized access, or provide a security credential for any level of access to a covered facility or resource;

“(iii) a review of any efforts that the Screening Coordination Office of the Department of Homeland Security has undertaken or plans to undertake to harmonize or standardize background check, access control, or credentialing requirements for critical infrastructure and key resource protection programs overseen by the Department; and

“(iv) recommendations, developed in consultation with appropriate stakeholders, regarding—

“(I) enhancing the interoperability of security credentials across critical infrastructure and key resource protection programs;

“(II) eliminating the need for redundant background checks or credentials across existing critical infrastructure and key resource protection programs;

“(III) harmonizing, where appropriate, the standards for identifying potentially disqualifying criminal offenses and the weight assigned to minor, nonviolent, or juvenile offenses in adjudicating the results of a completed background check; and

“(IV) the development of common, risk-based standards with respect to the background check, access control, and security credentialing requirements for critical infrastructure and key resource protection programs.

“(g) DEFINITIONS.—In this section—

“(1) the term ‘appropriate committees of Congress’ means—

“(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

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

“(C) the Permanent Select Committee on Intelligence, the Committee on Oversight and Government Reform, and the Committee on Homeland Security of the House of Representatives; and

“(2) the term ‘Performance Accountability Council’ means the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103) [50 U.S.C. 3161 note], or any successor thereto.”

[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)(7) to section 1086 of Pub. L. 114-92, set out above, is effective as of Nov. 25, 2015, and as if included in Pub. L. 114-92 as enacted.]

PERSONNEL SECURITY

Pub. L. 113-66, div. A, title IX, §907, Dec. 26, 2013, 127 Stat. 818, as amended by Pub. L. 115-91, div. A, title X, §1051(s)(1), Dec. 12, 2017, 131 Stat. 1566, provided that:

“(a) COMPARATIVE ANALYSIS.—

“(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 26, 2013], the Secretary of Defense shall, acting through the Director of Cost Assessment and Program Evaluation and in consultation with the Director of the Office of Management and Budget, submit to the appropriate committees of Congress a report setting forth a comprehensive analysis comparing the quality, cost, and timeliness of personnel security clearance investigations and reinvestigations for employees and contractor personnel of the Department of Defense that are conducted by the Office of Personnel Management with the quality, cost, and timeliness of personnel security clearance investigations and reinvestigations for such personnel that are conducted by components of the Department of Defense.

“(2) ELEMENTS OF ANALYSIS.—The analysis under paragraph (1) shall do the following:

“(A) Determine and compare, for each of the Office of Personnel Management and the components of the Department that conduct personnel security investigations as of the date of the analysis, the

quality, cost, and timeliness associated with personnel security investigations and reinvestigations of each type and level of clearance, and identify the elements that contribute to such cost, schedule, and performance.

“(B) Identify mechanisms for permanently improving the transparency of the cost structure of personnel security investigations and reinvestigations.

“(b) PERSONNEL SECURITY FOR DEPARTMENT OF DEFENSE EMPLOYEES AND CONTRACTORS.—If the Secretary of Defense determines that the current approach for obtaining personnel security investigations and reinvestigations for employees and contractor personnel of the Department of Defense is not the most efficient and effective approach for the Department, the Secretary shall develop a plan, by not later than October 1, 2014, for the transition of personnel security investigations and reinvestigations to the approach preferred by the Secretary.

“(c) STRATEGY FOR MODERNIZING PERSONNEL SECURITY.—

“(1) STRATEGY REQUIRED.—Not later than 180 days after the date of the enactment of this Act [Dec. 26, 2013], the Secretary of Defense, the Director of National Intelligence, and the Director of the Office of Management and Budget shall jointly develop, implement, and provide to the appropriate committees of Congress a strategy to modernize all aspects of personnel security for the Department of Defense with the objectives of improving quality, providing for continuous monitoring, decreasing unauthorized disclosures of classified information, lowering costs, increasing efficiencies, and enabling and encouraging reciprocity.

“(2) CONSIDERATION OF ANALYSIS.—In developing the strategy under paragraph (1), the Secretary and the Directors shall consider the results of the analysis required by subsection (a) and the results of any ongoing reviews of recent unauthorized disclosures of national security information.

“(3) METRICS.—In developing the strategy required by paragraph (1), the Secretary and the Directors shall jointly establish metrics to measure the effectiveness of the strategy in meeting the objectives specified in that paragraph.

“(4) ELEMENTS.—In developing the strategy required by paragraph (1), the Secretary and the Directors shall address issues including but not limited to the following:

“(A) Elimination of manual or inefficient processes in investigations and reinvestigations for personnel security, wherever practicable, and automating and integrating the elements of the investigation and adjudication processes, including in the following:

- “(i) The clearance application process.
- “(ii) Investigation case management.
- “(iii) Adjudication case management.

“(iv) Investigation methods for the collection, analysis, storage, retrieval, and transfer of data and records from investigative sources and between any case management systems.

“(v) Records management for hiring and clearance decisions.

“(B) Elimination or reduction, where possible, of the use of databases and information sources that cannot be accessed and processed automatically electronically, or modification of such databases and information sources, if appropriate and cost-effective, to enable electronic access and processing.

“(C) Access and analysis of government, publicly available, and commercial data sources, including social media, that provide independent information pertinent to adjudication guidelines and termination standards to improve quality and timeliness, and reduce costs, of investigations and reinvestigations.

“(D) Use of government-developed and commercial technology for continuous monitoring and

evaluation of government and commercial data sources that can identify and flag information pertinent to hiring and clearance determinations.

“(E) Standardization of forms used for routine reporting required of cleared personnel (such as travel, foreign contacts, and financial disclosures) and use of continuous monitoring technology to access databases containing such reportable information to independently obtain and analyze reportable data and events.

“(F) Establishment of an authoritative central repository of personnel security information that is accessible electronically at multiple levels of classification and eliminates technical barriers to rapid access to information necessary for eligibility determinations and reciprocal recognition thereof, including the ability to monitor the status of an individual and any events related to the continued eligibility of such individual for employment or clearance during intervals between investigations.

“(G) Elimination or reduction of the scope of, or alteration of the schedule for, periodic reinvestigations of cleared personnel, when such action is appropriate in light of the information provided by continuous monitoring or evaluation technology.

“(H) Electronic integration of personnel security processes and information systems with insider threat detection and monitoring systems, and pertinent law enforcement, counterintelligence and intelligence information, for threat detection and correlation, including those processes and systems operated by components of the Department of Defense for purposes of local security, workforce management, or other related purposes.

“(5) RISK-BASED MONITORING.—The strategy required by paragraph (1) shall—

“(A) include the development of a risk-based approach to monitoring and reinvestigation that prioritizes which cleared individuals shall be subject to frequent reinvestigations and random checks, such as the personnel with the broadest access to classified information or with access to the most sensitive classified information, including information technology specialists or other individuals with such broad access commonly known as ‘super users’;

“(B) ensure that if the system of continuous monitoring for all cleared individuals described in paragraph (4)(D) is implemented in phases, such system shall be implemented on a priority basis for the individuals prioritized under subparagraph (A); and

“(C) ensure that the activities of individuals prioritized under subparagraph (A) shall be monitored especially closely.

“(d) RECIPROCITY OF CLEARANCES.—The Secretary of Defense and the Director of National Intelligence shall jointly ensure the reciprocity of personnel security clearances among positions requiring personnel holding secret, top secret, or sensitive compartmented information clearances, to the maximum extent feasible consistent with national security requirements.

“(e) COMPTROLLER GENERAL REVIEW.—

“(1) REVIEW REQUIRED.—Not later than 150 days after the date of the enactment of this Act [Dec. 26, 2013], the Comptroller General of the United States shall carry out a review of the personnel security process.

“(2) OBJECTIVE OF REVIEW.—The objective of the review required by paragraph (1) shall be to identify the following:

“(A) Differences between the metrics used by the Department of Defense and other departments and agencies that grant security clearances in granting reciprocity for security clearances, and the manner in which such differences can be harmonized.

“(B) The extent to which existing Federal Investigative Standards are relevant, complete, and sufficient for guiding agencies and individual investigators as they conduct their security clearance background investigations.

“(C) The processes agencies have implemented to ensure quality in the security clearance background investigation process.

“(D) The extent to which agencies have developed and implemented outcome-focused performance measures to track the quality of security clearance investigations and any insights from these measures.

“(E) The processes agencies have implemented for resolving incomplete or subpar investigations, and the actions taken against government employees and contractor personnel who have demonstrated a consistent failure to abide by quality assurance measures.

“(3) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General shall submit to the appropriate committees of Congress a report on the results of the review required by paragraph (1).

“(f) TASK FORCE ON RECORDS ACCESS FOR SECURITY CLEARANCE BACKGROUND INVESTIGATIONS.—

“(1) ESTABLISHMENT.—The Suitability and Security Clearance Performance Accountability Council, as established by Executive Order No. 13467 [50 U.S.C. 3161 note], shall convene a task force to examine the different policies and procedures that determine the level of access to public records provided by State and local authorities in response to investigative requests by Federal Government employees or contracted employees carrying out background investigations to determine an individual’s suitability for access to classified information or secure government facilities.

“(2) MEMBERSHIP.—The members of the task force shall include, but need not be limited to, the following:

“(A) The Chair of the Suitability and Security Clearance Performance and Accountability Council, who shall serve as chair of the task force.

“(B) A representative from the Office of Personnel Management.

“(C) A representative from the Office of the Director of National Intelligence.

“(D) A representative from the Department of Defense responsible for administering security clearance background investigations.

“(E) Representatives from Federal law enforcement agencies within the Department of Justice and the Department of Homeland Security involved in security clearance background investigations.

“(F) Representatives from State and local law enforcement agencies, including—

“(i) agencies in rural areas that have limited resources and less than 500 officers; and

“(ii) agencies that have more than 1,000 officers and significant technological resources.

“(G) A representative from Federal, State, and local law enforcement associations involved with security clearance background administrative actions and appeals.

“(H) Representatives from Federal, State, and local judicial systems involved in the sharing of records to support security clearance background investigations.

“(3) INITIAL MEETING.—The task force shall convene its initial meeting not later than 45 days after the date of the enactment of this Act [Dec. 26, 2013].

“(4) DUTIES.—The task force shall do the following:

“(A) Analyze the degree to which State and local authorities comply with investigative requests made by Federal Government employees or contractor employees carrying out background investigations to determine an individual’s suitability for access to classified information or secure government facilities, including the degree to which investigative requests are required but never formally requested.

“(B) Analyze limitations on the access to public records provided by State and local authorities in response to investigative requests by Federal Gov-

ernment employees and contractor employees described in subparagraph (A), including, but not be limited to, limitations relating to budget and staffing constraints on State and local authorities, any procedural and legal obstacles impairing Federal access to State and local law enforcement records, or inadequate investigative procedural standards for background investigators.

“(C) Provide recommendations for improving the degree of cooperation and records-sharing between State and local authorities and Federal Government employees and contractor employees described in subparagraph (A).

“(5) REPORT.—Not later than 120 days after the date of the enactment of this Act, the task force shall submit to the appropriate committees of Congress a report setting forth a detailed statement of the findings and conclusions of the task force pursuant to this subsection, together with the recommendations of the task force for such legislative or administrative action as the task force considers appropriate.

“(g) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ‘appropriate committees of Congress’ means—

“(1) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate; and

“(2) the Committee on Armed Services, the Committee on Oversight and Government Reform, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives.”

REQUIRED NOTIFICATION WHENEVER MEMBERS OF THE ARMED FORCES ARE COMPLETING STANDARD FORM 86 OF THE QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Pub. L. 113–66, div. A, title XVII, §1747, Dec. 26, 2013, 127 Stat. 983, provided that:

“(a) NOTIFICATION OF POLICY.—Whenever a member of the Armed Forces is required to complete Standard Form 86 of the Questionnaire for National Security Positions in connection with an application, investigation, or reinvestigation for a security clearance, the member shall be notified of the policy described in subsection (b) regarding question 21 of such form.

“(b) POLICY DESCRIBED.—The policy referred to in subsection (a) is the policy of instructing an individual to answer ‘no’ to question 21 of Standard Form 86 of the Questionnaire for National Security Positions with respect to consultation with a health care professional if—

“(1) the individual is a victim of a sexual assault; and

“(2) the consultation occurred with respect to an emotional or mental health condition strictly in relation to the sexual assault.”

DEADLINE FOR PRESCRIBING PROCESS FOR PRIORITIZING BACKGROUND INVESTIGATIONS FOR SECURITY CLEARANCES

Pub. L. 106–398, §1 [[div. A], title X, §1072(c)], Oct. 30, 2000, 114 Stat. 1654, 1654A–277, provided that the process required by subsec. (a) of this section for expediting the completion of security clearance background investigations was to be prescribed by Jan. 1, 2001.

Executive Documents

EX. ORD. NO. 13869. TRANSFERRING RESPONSIBILITY FOR BACKGROUND INVESTIGATIONS TO THE DEPARTMENT OF DEFENSE

Ex. Ord. No. 13869, Apr. 24, 2019, 84 F.R. 18125, provided:

By the power vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Findings and Purpose.* Section 925 of the National Defense Authorization Act for Fiscal Year

2018 (10 U.S.C. 1564 note) provides that the Secretary of Defense has the authority to conduct security, suitability, and credentialing background investigations for Department of Defense personnel and requires the Secretary, in consultation with the Director of the Office of Personnel Management, to provide for a phased transition to the Department of Defense of the conduct of such investigations conducted by the National Background Investigations Bureau (NBIB). Implementing that legislative mandate while retaining the benefit of economies of scale in addressing the Federal Government's background investigations workload, avoiding unnecessary risk, promoting the ongoing alignment of efforts with respect to vetting Federal employees and contractors, and facilitating needed reforms in this critical area requires that the primary responsibility for conducting background investigations Government-wide be transferred from the Office of Personnel Management to the Department of Defense.

SEC. 2. *Transfer or Delegation of Background Investigation Functions; Further Amendments to Executive Order 13467 of June 30, 2008, as amended.* [Amended Ex. Ord. No. 13467, set out as a note under section 3161 of Title 50, War and National Defense.]

SEC. 3. *Amendment to Executive Order 12171 of November 18, 1979, as amended.*

(a) *Determinations.* Pursuant to section 7103(b)(1) of title 5, United States Code, the DCSA, previously known as the DSS, is hereby determined to have as a primary function intelligence, counterintelligence, investigative, or national security work. It is further determined that chapter 71 of title 5, United States Code, cannot be applied to the DCSA in a manner consistent with national security requirements and considerations.

(b) *Exclusion.* [Amended Ex. Ord. No. 12171, set out as a note under section 7103 of Title 5, Government Organization and Employees.]

SEC. 4. *Conforming References to the Defense Security Service and the Defense Counterintelligence and Security Agency.* Any reference to the Defense Security Service or NBIB in any Executive Order or other Presidential document that is in effect on the day before the date of this order shall be deemed or construed to be a reference to the Defense Counterintelligence and Security Agency or any other entity that the Secretary of Defense names, consistent with section 2(b)(i) of Executive Order 13467, and agencies whose regulations, rules, or other documents reference the Defense Security Service or NBIB shall revise any such respective regulations, rules, or other documents as soon as practicable to update them for consistency with this order.

SEC. 5. *Review of Vetting Policies.* No later than July 24, 2019, the Council Principals identified in section 2.4(b) of Executive Order 13467 shall review the laws, regulations, Executive Orders, and guidance relating to the Federal Government's vetting of Federal employees and contractors and shall submit to the President, through the Chair of the Council, a report recommending any appropriate legislative, regulatory, or policy changes, including any such changes to civil service regulations or policies, Executive Order 13467 or Executive Order 13488 [5 U.S.C. 7301 note].

SEC. 6. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP.

§ 1564a. Counterintelligence polygraph program

(a) **AUTHORITY FOR PROGRAM.**—The Secretary of Defense may carry out a program for the administration of counterintelligence polygraph examinations to persons described in subsection (b). The program shall be conducted in accordance with the standards specified in subsection (e).

(b) **PERSONS COVERED.**—Except as provided in subsection (d), the following persons are subject to this section:

(1) With respect to persons whose duties are described in subsection (c)—

(A) military and civilian personnel of the Department of Defense;

(B) personnel of defense contractors;

(C) persons assigned or detailed to the Department of Defense; and

(D) applicants for a position in the Department of Defense.

(2) A person who is—

(A) a national of the United States (as such term is defined in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101)) and also a national of a foreign state; and

(B) either—

(i) a civilian employee or contractor who requires access to classified information; or

(ii) a member of the armed forces who requires access to classified information.

(c) **COVERED TYPES OF DUTIES.**—The Secretary of Defense may provide, under standards established by the Secretary, that a person described in subsection (b)(1) is subject to this section if that person's duties involve—

(1) access to information that—

(A) has been classified at the level of top secret; or

(B) is designated as being within a special access program under section 4.4(a) of Executive Order No. 12958 (or a successor Executive order); or

(2) assistance in an intelligence or military mission in a case in which the unauthorized disclosure or manipulation of information, as determined under standards established by the Secretary of Defense, could reasonably be expected to—

(A) jeopardize human life or safety;

(B) result in the loss of unique or uniquely productive intelligence sources or methods vital to United States security; or

(C) compromise technologies, operational plans, or security procedures vital to the strategic advantage of the United States and its allies.

(d) **EXCEPTIONS FROM COVERAGE FOR CERTAIN INTELLIGENCE AGENCIES AND FUNCTIONS.**—This section does not apply to the following persons:

(1) A person assigned or detailed to the Central Intelligence Agency or to an expert or consultant under a contract with the Central Intelligence Agency.

(2) A person who is—

(A) employed by or assigned or detailed to the National Security Agency;

(B) an expert or consultant under contract to the National Security Agency;