(7) a description of the implementation of quality control procedures and mechanisms for monitoring compliance with quality control procedures.

TITLE III—SECURITY CLEARANCES

SEC. 3001. SECURITY CLEARANCES.

(a) DEFINITIONS.—In this section:

(1) The term "agency" means—

(A) an executive agency (as that term is defined in section 105 of title 5, United States Code);

(B) a military department (as that term is defined in section 102 of title 5, United States Code); and

(C) an element of the intelligence community.

(2) The term "authorized investigative agency" means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(3) The term "authorized adjudicative agency" means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term "highly sensitive program" means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)); or

(ii) other information commonly referred to as "sensitive compartmented information".

(5) The term "current investigation file" means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

(A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;

(B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance; and

(C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.

(6) The term "personnel security investigation" means any investigation required for the purpose of determining the eligibility of any military, civilian, or government contractor personnel to access classified information.

(7) The term "periodic reinvestigations" means investigations conducted for the purpose of updating a previously completed background investigation—

(A) every 5 years in the case of a top secret clearance or access to a highly sensitive program;

(B) every 10 years in the case of a secret clearance; or

(C) every 15 years in the case of a Confidential Clearance.

(8) The term "appropriate committees of Congress" means—

(A) the Permanent Select Committee on Intelligence and the Committees on Armed Services, Homeland Security, Government Reform, and the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence and the Committees on Armed Services, Homeland Security and Governmental Affairs, and the Judiciary of the Senate.

(b) SELECTION OF ENTITY.—Not later than 90 days after the date of the enactment of this Act, the President shall select a single department, agency, or element of the executive branch to be responsible for—

(1) directing day-to-day oversight of investigations and adjudications for personnel security clearances, including for highly sensitive programs, throughout the United States Government;

(2) developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures;

(3) serving as the final authority to designate an authorized investigative agency or authorized adjudicative agency;

(4) ensuring reciprocal recognition of access to classified information among the agencies of the United States Government, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of security clearances and access to highly sensitive programs pursuant to subsection (d);

(5) ensuring, to the maximum extent practicable, that sufficient resources are available in each agency to achieve clearance and investigative program goals; and

(6) reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and granting of clearances.

(c) PERFORMANCE OF SECURITY CLEARANCE INVESTIGATIONS.—(1) Notwithstanding any other provision of law, not later than 180 days after the date of the enactment of this Act, the President shall, in consultation with the head of the entity selected pursuant to subsection (b), select a single agency of the executive branch to conduct, to the maximum extent practicable, security clearance investigations of employees and contractor personnel of the United States Government who require access to classified information and to provide and maintain all security clearances of such employees and contractor personnel. The head of the entity selected pursuant to subsection (b) may designate other agencies to conduct such investiga-

tions if the head of the entity selected pursuant to subsection (b) considers it appropriate for national security and efficiency purposes.

(2) The agency selected under paragraph (1) shall—

(A) take all necessary actions to carry out the requirements of this section, including entering into a memorandum of understanding with any agency carrying out responsibilities relating to security clearances or security clearance investigations before the date of the enactment of this Act;

(B) as soon as practicable, integrate reporting of security clearance applications, security clearance investigations, and determinations of eligibility for security clearances, with the database required by subsection (e); and

(C) ensure that security clearance investigations are conducted in accordance with uniform standards and requirements established under subsection (b), including uniform security questionnaires and financial disclosure requirements.

(d) RECIPROCITY OF SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—(1) All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies.

(2) All security clearance background investigations initiated by an authorized investigative agency shall be transferable to any other authorized investigative agency.

(3)(A) An authorized investigative agency or authorized adjudicative agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination) that exceed requirements specified in Executive Orders establishing security requirements for access to classified information without the approval of the head of the entity selected pursuant to subsection (b).

(B) Notwithstanding subparagraph (A), the head of the entity selected pursuant to subsection (b) may establish such additional requirements as the head of such entity considers necessary for national security purposes.

(4) An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual where a current investigation or clearance of equal level already exists or has been granted by another authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may disallow the reciprocal recognition of an individual security clearance by an agency under this section on a case-by-case basis if the head of the entity selected pursuant to subsection (b) determines that such action is necessary for national security purposes.

(6) The head of the entity selected pursuant to subsection (b) shall establish a review procedure by which agencies can seek review of actions required under this section.

(e) DATABASE ON SECURITY CLEARANCES.—(1) Not later than 12 months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall, in cooperation with the heads of the entities selected pursuant to subsections (b) and (c), establish and commence operating and maintaining an integrated, secure, database into which appropriate data relevant to the granting, denial, or revocation of a security clearance or access pertaining to

military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.

(2) The database under this subsection shall function to integrate information from existing Federal clearance tracking systems from other authorized investigative and adjudicative agencies into a single consolidated database.

(3) Each authorized investigative or adjudicative agency shall check the database under this subsection to determine whether an individual the agency has identified as requiring a security clearance has already been granted or denied a security clearance, or has had a security clearance revoked, by any other authorized investigative or adjudicative agency.

(4) The head of the entity selected pursuant to subsection (b) shall evaluate the extent to which an agency is submitting information to, and requesting information from, the database under this subsection as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may authorize an agency to withhold information about certain individuals from the database under this subsection if the head of the entity considers it necessary for national security purposes.

(f) EVALUATION OF USE OF AVAILABLE TECHNOLOGY IN CLEARANCE INVESTIGATIONS AND ADJUDICATIONS.—(1) The head of the entity selected pursuant to subsection (b) shall evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for a security clearance.

(2) The evaluation shall assess the application of the technologies described in paragraph (1) for—

(A) granting interim clearances to applicants at the secret, top secret, and special access program levels before the completion of the appropriate full investigation;

(B) expediting investigations and adjudications of security clearances, including verification of information submitted by the applicant;

(C) ongoing verification of suitability of personnel with security clearances in effect for continued access to classified information;

(D) use of such technologies to augment periodic reinvestigations;

(E) assessing the impact of the use of such technologies on the rights of applicants to verify, correct, or challenge information obtained through such technologies; and

(F) such other purposes as the head of the entity selected pursuant to subsection (b) considers appropriate.

(3) An individual subject to verification utilizing the technology described in paragraph (1) shall be notified of such verification, shall provide consent to such use, and shall have access to data being verified in order to correct errors or challenge information the individual believes is incorrect.

(4) Not later than one year after the date of the enactment of this Act, the head of the entity selected pursuant to subsection (b) shall submit to the President and the appropriate committees of

Congress a report on the results of the evaluation, including recommendations on the use of technologies described in paragraph (1).

(g) REDUCTION IN LENGTH OF PERSONNEL SECURITY CLEARANCE PROCESS.—(1) The head of the entity selected pursuant to subsection (b) shall, within 90 days of selection under that subsection, develop, in consultation with the appropriate committees of Congress and each authorized adjudicative agency, a plan to reduce the length of the personnel security clearance process.

(2)(A) To the extent practical the plan under paragraph (1) shall require that each authorized adjudicative agency make a determination on at least 90 percent of all applications for a personnel security clearance within an average of 60 days after the date of receipt of the completed application for a security clearance by an authorized investigative agency. Such 60-day average period shall include—

(i) a period of not longer than 40 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 20 days to complete the adjudicative phase of the clearance review.

(B) Determinations on clearances not made within 60 days shall be made without delay.

(3)(A) The plan under paragraph (1) shall take effect 5 years after the date of the enactment of this Act.

(B) During the period beginning on a date not later than 2 years after the date after the enactment of this Act and ending on the date on which the plan under paragraph (1) takes effect, each authorized adjudicative agency shall make a determination on at least 80 percent of all applications for a personnel security clearance pursuant to this section within an average of 120 days after the date of receipt of the application for a security clearance by an authorized investigative agency. Such 120-day average period shall include—

(i) a period of not longer than 90 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 30 days to complete the adjudicative phase of the clearance review.

(h) REPORTS.—(1) Not later than February 15, 2006, and annually thereafter through 2011, the head of the entity selected pursuant to subsection (b) shall submit to the appropriate committees of Congress a report on the progress made during the preceding year toward meeting the requirements of this section.

(2) Each report shall include, for the period covered by such report—

(A) the periods of time required by the authorized investigative agencies and authorized adjudicative agencies for conducting investigations, adjudicating cases, and granting clearances, from date of submission to ultimate disposition and notification to the subject and the subject's employer;

(B) a discussion of any impediments to the smooth and timely functioning of the requirements of this section; and

(C) such other information or recommendations as the head of the entity selected pursuant to subsection (b) considers appropriate.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary for fiscal year 2005 and each fiscal year thereafter for the implementation, maintenance, and operation of the database required by subsection (e).

TITLE IV—TRANSPORTATION SECURITY

Subtitle A—National Strategy for Transportation Security

SEC. 4001. NATIONAL STRATEGY FOR TRANSPORTATION SECURITY.

(a) IN GENERAL.—Section 114 of title 49, United States Code, is amended by adding at the end the following:

"(t) TRANSPORTATION SECURITY STRATEGIC PLANNING.—

"(1) IN GENERAL.—The Secretary of Homeland Security shall develop, prepare, implement, and update, as needed—

"(A) a National Strategy for Transportation Security; and

"(B) transportation modal security plans.

"(2) ROLE OF SECRETARY OF TRANSPORTATION.—The Secretary of Homeland Security shall work jointly with the Secretary of Transportation in developing, revising, and updating the documents required by paragraph (1).

"(3) CONTENTS OF NATIONAL STRATEGY FOR TRANSPORTATION SECURITY.—The National Strategy for Transportation Security shall include the following:

"(A) An identification and evaluation of the transportation assets in the United States that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces, including modal security plans for aviation, bridge and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail, mass transit, over-the-road bus, and other public transportation infrastructure assets that could be at risk of such an attack or disruption.

"(B) The development of risk-based priorities across all transportation modes and realistic deadlines for addressing security needs associated with those assets referred to in subparagraph (A).

"(C) The most appropriate, practical, and cost-effective means of defending those assets against threats to their security.

"(D) A forward-looking strategic plan that sets forth the agreed upon roles and missions of Federal, state, regional, and local authorities and establishes mechanisms for encouraging private sector cooperation and participation in the implementation of such plan.

"(E) A comprehensive delineation of response and recovery responsibilities and issues regarding threatened and executed acts of terrorism within the United States.

"(F) A prioritization of research and development objectives that support transportation security needs, giving a higher priority to research and development directed toward protecting vital transportation assets.