To reform classification and security clearance processes throughout the Federal Government and, within the Department of Homeland Security, to establish an effective and transparent process for the designation, investigation, adjudication, denial, suspension, and revocation of security clearances, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES
JULY 29, 2014

Mr. THOMPSON of Mississippi introduced the following bill; which was referred to the Committee on Oversight and Government Reform, and in addition to the Committees on Homeland Security, Select Intelligence (Permanent Select), and the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

A BILL
To reform classification and security clearance processes throughout the Federal Government and, within the Department of Homeland Security, to establish an effective and transparent process for the designation, investigation, adjudication, denial, suspension, and revocation of security clearances, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,
1 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Clearance and Over-Classification Reform and Reduction
4 Act” or the “CORRECT Act”.

5 (b) TABLE OF CONTENTS.—The table of contents for
6 this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—REFORMS TO CLASSIFICATION AND CLEARANCE
PROCESSES

Subtitle A—Reducing Over-Classification

Sec. 101. Trend information on classified information and third evaluations.
Sec. 102. Uniformity in sampling.
Sec. 103. Ten percent reduction in holdings of classified information.
Sec. 104. Status update on efforts at reducing holdings of classified information.
Sec. 105. Report.
Sec. 106. Public Interest Declassification Board enhancements.
Sec. 107. Classification designation training.
Sec. 108. Reducing over-classification guidance.

Subtitle B—Governmentwide Reforms

Sec. 111. Sense of Congress.
Sec. 112. Report on certain designations.
Sec. 113. Transparency and accountability in personnel security investigations.
Sec. 114. Continuous evaluation programs and insider threat programs.
Sec. 115. Mitigating factors in the context of a continuous evaluation program
or insider threat program.
Sec. 116. Appeal to the Merit Systems Protection Board.
Sec. 117. Automated or nongovernmental adjudication prohibited.
Sec. 118. Report on media contacts policy for intelligence personnel.

TITLE II—DEPARTMENT OF HOMELAND SECURITY CLEARANCE
PROCESS REFORMS

Subtitle A—Designation

Sec. 201. Designation of national security sensitive and public trust positions.
Sec. 203. Review of position designations.

Subtitle B—Investigation

Sec. 211. Investigation services provider performance.
Sec. 212. Metrics.

Subtitle C—Adjudication
Sec. 221. Uniform adjudication standards.

Subtitle D—Denial, Suspension, Revocation, and Appeal

Sec. 231. Uniform revocation criteria and procedures.
Sec. 232. Annual reporting.
Sec. 233. Final appeals panel.

Subtitle E—Miscellaneous Provisions

Sec. 241. Intelligence Reform and Terrorism Prevention Act of 2004 review and security clearance reciprocity.
Sec. 243. Penalties for falsification relating to an investigation file.

SEC. 2. DEFINITIONS.

In this Act:

(1) CHIEF SECURITY OFFICER.—The term “Chief Security Officer” means the Classified Information Advisory Officer of the Department of Homeland Security (identified and designated pursuant to section 210F of the Homeland Security Act of 2002 (6 U.S.C. 124m)).

(2) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT TERMS.—The terms “agency”, “authorized investigative agency”, “authorized adjudicative agency”, “current investigation file”, “periodic reinvestigations”, and “personnel security investigation” have the meanings given those terms in section 3001(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(a)).

(3) INVESTIGATION SERVICE PROVIDER.—The term “investigation service provider” means the Office of Personnel Management and any other entity
that undertakes investigative services, including
criminal record checks, financial record checks, field
interviews, employment review, and education
verifications, for an investigation file for a national
security position.

(4) NATIONAL SECURITY POSITION.—The term
“national security position” has the meaning given
that term in section 732.102 of title 5, Code of Fed-
eral Regulations.

TITLE I—REFORMS TO CLASSI-
FICATION AND CLEARANCE
PROCESSES

Subtitle A—Reducing Over-
Classification

SEC. 101. TREND INFORMATION ON CLASSIFIED INFORMA-
TION AND THIRD EVALUATIONS.

Subsection (b) of section 6 of the Reducing Over-
Classification Act (50 U.S.C. 3161 note; Public Law 111–
258) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph

(A)—

(i) by striking “2016” and inserting

“2019”; and
(ii) by striking “no less than two” and inserting “not fewer than three’’;

(B) in subparagraph (A), by striking “and” at the end;

(C) in subparagraph (B), by striking the period at the end and inserting “; and”; and

(D) by adding after subparagraph (B) the following new subparagraph:

“(C) beginning with the second evaluation under paragraph (2)(B), to assess, with respect to subparagraph (A) of this paragraph, the degree to which the incentives for accurate classification decisions referred to in subsection (a) have been utilized, and the extent to which the use of such incentives, including cash incentives or other alternative, non-cash awards, has improved the accuracy of original classification decisions or derivative classification decisions and a reduction in classified information.”;

(2) in paragraph (2), by adding at the end the following new subparagraph:

“(C) THIRD EVALUATIONS.—Each third evaluation required by paragraph (1) shall review progress made since the second evaluation and the adequacy of the records to support each
self-inspection program determination in ac-
cordance with subsection (c), and assess such
department or agency’s procedures and activi-
ties regarding classification challenges. Specifi-
cally, each third evaluation shall—

“(i)(I) assess implementation of pro-
cedures by such department or agency to
encourage authorized holders of classified
information, including authorized holders
outside the classifying agency, to challenge
the classification of information that they
believe is improperly classified or unclassi-
fied, as required by section 1.8 of Execu-
tive Order 13526 (50 U.S.C. 3161 note) or
successor order, and the degree to which
such department or agency makes each au-
thorized holder of classified information
aware of the procedures and encourages
such holders to challenge the classification
of information that they believe is improp-
erly classified or unclassified; and

“(II) to the extent practicable, review
data reflecting the disposition of challenges
received by such department or agency, in-
cluding how often such challenges resulted
in a change in classification;

“(ii) review the degree to which infor-
mation that was declassified was deter-
mined by the agency to be of extraordinary
public interest that does not undermine the
national security of the United States, in-
cluding information on the number of na-
tional security positions (pursuant to sec-
tion 732 of title 5, Code of Federal Regu-
lations), by classification level, that are
designated within the agency during that
period; and

“(iii) shall be completed not later than
September 30, 2019.”; and

(3) in paragraph (3)(B)—

(A) in clause (i), by striking “and” at the
end;

(B) in clause (ii), by striking the period at
the end and inserting “; and”; and

(C) by adding after clause (ii) the following
new clause:

“(iii) information relating to the as-
essment required under paragraph
(1)(C).”.
SEC. 102. UNIFORMITY IN SAMPLING.

Section 6 of the Reducing Over-Classification Act (50 U.S.C. 3161 note; Public Law 111–258) is amended by adding at the end the following new subsection:

“(c) UNIFORMITY IN SAMPLING.—The President, acting through the Director of the Information Security Oversight Office, shall issue a standardized sampling technique for department and agency self-inspection programs as required pursuant to Executive Order 13526 (50 U.S.C. 3161 note) in order to address any vulnerabilities in such programs.”.

SEC. 103. TEN PERCENT REDUCTION IN HOLDINGS OF CLASSIFIED INFORMATION.

Section 6 of the Reducing Over-Classification Act (50 U.S.C. 3161 note; Public Law 111–258), as amended by section 102 of this Act, is further amended by adding at the end the following new subsection:

“(d) TEN PERCENT REDUCTION IN HOLDING OF CLASSIFIED INFORMATION.—The President shall establish goals for reducing, by the date that is not later than five years after the date of the enactment of this subsection, classified information, through declassification and improved original and derivative classification decisionmaking, by not less than ten percent as compared to the amount of such information as of the day before such date. For purposes of this subsection, classified informa-
tion that would otherwise be declassified pursuant to Executive Order 13526 (50 U.S.C. 3161 note) shall not count towards such ten percent requirement.”.

SEC. 104. STATUS UPDATE ON EFFORTS AT REDUCING HOLDINGS OF CLASSIFIED INFORMATION.

Section 704(d)(1) of the Public Interest Declassification Act of 2000 (50 U.S.C. 3161 note; Public Law 106–567) is amended by striking the period and inserting “and information on the status of efforts, to the extent practicable on an agency-by-agency basis, at reducing the holding of classified information pursuant to section 6(d) of the Reducing Over-Classification Act (50 U.S.C. 3161 note; Public Law 111–258).”.

SEC. 105. REPORT.

Section 6 of the Reducing Over-Classification Act (50 U.S.C. 3161 note; Public Law 111–258), as amended by sections 102 and 103 of this Act, is further amended by adding at the end the following new subsection:

“(e) REPORT.—The Inspector General of each department or agency of the United States with an officer or employee who is authorized to make original and derivative classification decisions shall submit to the appropriate entities (as such term is defined in subsection (b)(4)) a report relating to progress accomplished under subsections (c) and (d).”.
SEC. 106. PUBLIC INTEREST DECLASSIFICATION BOARD

ENHANCEMENTS.

(a) Reviews of Classification Guidance.—Sub-
sections (a) and (b) of section 704 of the Public Interest
Declassification Act of 2000 (50 U.S.C. 3161 note; Public
Law 106–567) are amended to read as follows:

“(a) Agency Declassification Programs and
Classification Guidance.—

“(1) Declassification programs.—

“(A) Report.—The head of any agency
with the authority under an Executive order to
classify information shall annually provide to
the Board, the Select Committee on Intelligence
of the Senate, and the Permanent Select Com-
mittee on Intelligence of the House of Rep-
resentatives a summary briefing and report on
the progress and plans of such agency in the
declassification of national security information.

“(B) Contents.—Each briefing and re-
port required under subparagraph (A) shall—

“(i) cover the declassification goals set
by statute, regulation, or policy, the
progress of the agency towards completing
such goals, and the planned goals and pri-
orities of the agency for its declassification
activities over the 2 fiscal years following
the report;

“(ii) give particular attention to
progress on the declassification of records
and materials that are of extraordinary
public interest to the people of the United
States; and

“(iii) include information on the dis-
position of recommendations regarding
Special Searches for Records of Extraor-
dinary Public Interest submitted pursuant
to section 704(c).

“(C) CONSOLIDATED REPORT.—The an-
nual briefing and report under paragraph (1)
for agencies within the Department of Defense,
including the military departments and the ele-
ments of the intelligence community (as defined
in section 3(4) of the National Security Act of
1947 (50 U.S.C. 3003(4))), shall be provided
on a consolidated basis.

“(2) REVIEW OF CLASSIFICATION GUIDANCE.—
The Board shall, on an ongoing basis, review classi-
ification guidance required pursuant to Executive
Order 13526 (50 U.S.C. 3161 note) or any suc-
cessor order utilized within each agency to assess—
“(A) the validity of the national security basis for each instruction in the classification guidance;

“(B) the clarity of each instruction within the classification guidance to ensure that only the minimum necessary information is classified; and

“(C) the feasibility of narrowing or eliminating any classification guidance that is unnecessary or obsolete.

“(3) PLAN FOR REVIEWING CLASSIFICATION GUIDANCE.—Not later than 90 days after the date of the enactment of the Clearance and Over-Classification Reform and Reduction Act, the Chairperson of the Board shall submit a multi-year plan for reviewing classification guidance utilized within each agency, with benchmarks for when and, to the extent practicable, which classification guidance will be reviewed and how the findings will be shared with the head of each agency and the inspector general of each agency.

“(4) RECOMMENDATIONS FOR HARMONIZING AND REDUCING CLASSIFICATION GUIDANCE.—Not later than one year after the date of the enactment of the Clearance and Over-Classification Reform and
Reduction Act, the Chairperson of the Board shall submit recommendations for harmonizing and reducing classification guidance across the Federal Government to the President.

“(b) RECOMMENDATIONS ON AGENCY DECLASSIFICATION PROGRAMS AND CLASSIFICATION GUIDANCE.—

“(1) IN GENERAL.—Upon reviewing classification guidance and discussing declassification plans and progress with an agency, the Board shall provide to the head of that agency, the Director of the Office of Management and Budget, and the Assistant to the President for National Security Affairs the written recommendations of the Board as to how the classification guidance and declassification program of the agency could be improved.

“(2) PUBLIC AVAILABILITY.—Not later than 60 days after the Board provides written recommendations to the head of an agency in accordance with paragraph (1), the Board shall make such recommendations public in accordance with subsection (k).”.

(b) STAFF AND DETAILLEES.—Subsection (f) of section 703 of such Act is amended to read as follows:

“(f) DIRECTOR AND STAFF.—
“(1) DIRECTOR.—The Chairperson of the Board, in accordance with rules agreed upon by the Board, shall appoint and fix the compensation of a Director, except that no rate of pay fixed under this paragraph may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

“(2) STAFF.—The Chairperson of the Board, in accordance with rules agreed upon by the Board, may appoint and fix the pay of personnel as may be necessary to enable the Board to carry out its functions.

“(3) APPLICABILITY OF CERTAIN CIVIL SERVICE LAWS.—The Director and staff may be appointed without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and may be paid without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates.

“(4) DETAILLEES.—Any employee of the Federal Government may be detailed to the Board with the agreement of, and without reimbursement to, the detailing agency, and such detail shall be without
interruption or loss of civil, military, or foreign service status or privilege.”.

(c) COMPENSATION AND TRAVEL EXPENSES.—Subsection (h) of section 703 of such Act is amended to read as follows:

“(h) COMPENSATION AND TRAVEL EXPENSES.—

“(1) COMPENSATION.—

“(A) CHAIRPERSON.—The Chairperson of the Board shall be compensated at the rate of pay payable for a position at level III of the Executive Schedule under section 5314 of title 5, United States Code.

“(B) MEMBERS.—Each member of the Board shall be compensated at a rate of pay payable for a position at level IV of the Executive Schedule under section 5315 of such title, for each day during which that member is engaged in the actual performance of the duties of the Board.

“(2) TRAVEL EXPENSES.—Members of the Board shall receive travel expenses, including per diem in lieu of subsistence, in accordance with applicable provisions under subchapter I of chapter 57 of title 5, United States Code.”.
(d) Public Meetings.—Section 704(c) of such Act is amended by adding at the end the following new paragraph:

“(3) In carrying out this subsection, the Board shall conduct public meetings on at least a semianual basis and publish in the Federal Register notice of such meetings.”.

(e) Extension of Sunset.—Subsection (b) of section 710 of such Act is amended by striking “2018” and inserting “2024”.

SEC. 107. CLASSIFICATION DESIGNATION TRAINING.

Section 7 of the Reducing Over-Classification Act (50 U.S.C. 3344; Public Law 111–258) is amended—

(1) in subsection (a), in the matter preceding paragraph (1)—

(A) in the first sentence, by inserting “, including computer-based training,” after “annual training”; and

(B) in the second sentence, by inserting “such” before “training”; and

(2) by adding at the end the following new subsection:

“(c) Recordkeeping.—The head of each Executive agency shall maintain records and make such records available to the inspector general of each such agency of
the extent to which training required under this section
is completed by each employee subject to such training.”.

SEC. 108. REDUCING OVER-CLASSIFICATION GUIDANCE.

The Secretary of Homeland Security shall develop
and disseminate to components of the Department of
Homeland Security and make available to other agencies
guidance on best practices and strategies to implement the
Reducing Over-Classification Act (Public Law 111–258),
as amended by this Act. Such guidance shall include infor-

(1) Administrative approaches, including the es-

tablishment of internal quarterly meetings and work-
ing groups to carry out the requirements of the Re-
ducing Over-Classification Act (Public Law 111–

(2) Consolidation of information security poli-
cies throughout an agency.

(3) Provision of training, including in-person
initial training and computer-based recurrent train-
ing, in accordance with section 7 of the Reducing
Over-Classification Act, as amended by section 105
of this Act.

(4) Adoption of uniform formats for the prepa-
ration, production, or publication of classified infor-

mation on the following:

(1) Administrative approaches, including the es-

tablishment of internal quarterly meetings and work-
ing groups to carry out the requirements of the Re-
ducing Over-Classification Act (Public Law 111–

(2) Consolidation of information security poli-
cies throughout an agency.

(3) Provision of training, including in-person
initial training and computer-based recurrent train-
ing, in accordance with section 7 of the Reducing
Over-Classification Act, as amended by section 105
of this Act.

(4) Adoption of uniform formats for the prepa-
ration, production, or publication of classified infor-

mation.
(5) Ways to encourage an authorized holder of classified information to challenge the classification of information that such holder believes is improperly classified or unclassified, as required by section 1.8 of Executive Order 13526 (50 U.S.C. 3161 note) or successor order.

**Subtitle B—Governmentwide Reforms**

**SEC. 111. SENSE OF CONGRESS.**

It is the sense of Congress that a position shall only be designated as a national security position if access to classified information is required or if that position—

(1) presents a risk of a material adverse effect on the national security (as described in section 732.201 of title 5, Code of Federal Regulations); and

(2) is determined to be a public trust position (as described in section 731.106 of title 5, Code of Federal Regulations).

**SEC. 112. REPORT ON CERTAIN DESIGNATIONS.**

(a) Report.—Not later than 6 months after the date of enactment of this Act and biannually thereafter, the head of each agency with the authority to designate a national security position shall submit to Congress a report that provides information regarding any national security
position for which access to classified materials is not re-
quired and the position is not determined to be a public
trust position (as described in section 731.106 of title 5,

(b) CONTENTS.—The report required under sub-
section (a) shall include—

(1) a description for the position, including spe-
cific information on duties and day-to-day oper-
ations;

(2) the history of the position’s national secu-
ruity position designation, including whether the posi-
tion is newly created or was transferred from an-
other department, division, or program;

(3) an explanation of the position’s national se-
curity position designation and whether responsibil-
ities have been added to the position to explain the
designation;

(4) an explanation of the national security im-
plications of the position;

(5) the advertising and recruitment mechanisms
used to fill the position;

(6) information on the individual who holds the
position, including as appropriate, information on
periods when the individual had previously held a
national security position; and
(7) demographic information on the individual who holds the position, including age, gender, race, ethnicity, employment status, and geographic location.

(c) PUBLIC REPORT.—The report required under subsection (a) shall be submitted in unclassified form and be made publicly available, but may include a classified annex for any sensitive or classified information if necessary.

SEC. 113. TRANSPARENCY AND ACCOUNTABILITY IN PERSONNEL SECURITY INVESTIGATIONS.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence and the Director of the Office of Personnel Management shall establish requirements for a uniform markings process to identify the investigation service provider that originated each piece of information in a current investigation file.

(b) UTILIZATION.—

(1) IN GENERAL.—Not later than 90 days after the establishment of the uniform markings process pursuant to subsection (a), investigation service providers shall utilize such uniform markings process and make available, upon request by the authorized
adjudicative agency, all documents in a current investigation file.

(2) EXCEPTION.—This subsection shall not apply to a personnel security investigation that an agency conducts using its own personnel, under delegated or statutory authority.

SEC. 114. CONTINUOUS EVALUATION PROGRAMS AND INSIDER THREAT PROGRAMS.

(a) FINDINGS.—Congress finds the following:

(1) The term “continuous evaluation” as defined in Executive Order 13467, means reviewing the background of an individual who has been determined to be eligible for access to classified information at any time during the period of eligibility.

(2) Since 1998, at least 10 continuous evaluation pilot studies have been carried out by Federal agencies to monitor the individuals with security clearances on an ongoing basis.

(3) The Department of Defense has conducted multiple continuous evaluation pilots since early 2002 and has more than one pilot that is ongoing as of July 1, 2014. By October 2014, the Department anticipates 100,000 people to be subject to continuous evaluation with the population steadily rising to 1 million by 2017.
(4) The Office of the Director of National Intelligence plans for all individuals with Top Secret clearances or higher to be subject to continuous evaluation by 2016.

(5) Since 2010, applicants submitting an application for a security clearance, the Standard Form 86, are required to consent to being monitored through continuous evaluation.

(6) In February 2014, the Office of Management and Budget issued a 120-day review of Federal employee suitability and contractor fitness determinations as well as security clearance procedures and recommended an accelerated timetable for an integrated solution or continuous evaluation program across all Federal agencies and security levels.

(7) In addition to continuous evaluation, some Federal agencies are establishing insider threat programs pursuant to Executive Order 13587 (50 U.S.C. 3161 note), which authorized the establishment of insider threat programs to, among other things, identify any Government or contracted employee that may have compromised national security through such employee’s work capacity.

(8) Continuous evaluation and insider threat programs are proliferating throughout the Federal
government without requirements for protections to ensure that such programs be designed and implemented in a manner that not only protects national security but also promotes fairness, transparency, and employee protections, including whistleblower protections.

(b) REQUIREMENTS.—Not later than 180 days after the date of enactment of this Act, the Privacy and Civil Liberties Oversight Board, established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee), shall publish in the Federal Register standards for the protection of national security and promotion of fairness, transparency, and employee protections, including safeguards to preserve the rights and confidentiality of whistleblowers with respect to the operation of a continuous evaluation program and the operation of an insider threat program by a Federal agency.

(c) CERTIFICATION.—

(1) IN GENERAL.—Not later than 90 days after the date of publication of the standards under subsection (b), the head of any agency that is operating a continuous evaluation program or insider threat program as of the date of the enactment of this Act shall—
(A) certify whether such program is in compliance with the standards established under subsection (b); and

(B) publish such certification in the Federal Register.

(2) SUSPENSION OR PROGRAM.—Any such head who certifies that a continuous evaluation program or insider threat program does not meet such standards or who fails to publish a certification of compliance pursuant to paragraph (1) shall suspend the program until such program is compliant and certification of compliance is published in the Federal Register.

(d) REPORT.—The head of any agency that is operating a continuous evaluation program or insider threat program as of the date of enactment of this Act shall annually submit to Congress a report that includes the following information:

(1) The number of individuals in the agency subject to the continuous evaluation program or insider threat program.

(2) The number of individuals in the agency whose eligibility for access to classified information was suspended or revoked as a result of information
acquired through the continuous evaluation program
or insider threat program.

(3) The total number of individuals in the agency
who are eligible to access classified information.

(4) Demographic information on each individual
whose eligibility for access to classified information
was changed as a result of information collected
through the continuous evaluation program or in-
sider threat program, including age, race, gender,
and ethnicity.

(5) A description of the mechanisms used to
conduct the evaluations, including how individuals
were selected, whether the evaluations were random-
ized, and if so, the nature of the randomization, in-
cluding the degree to which it was temporally ran-
domized and the degree to which the selection of in-
dividuals subject to the program was randomized.

(6) A description of the types of information
that were captured through the continuous evalu-
tion program or insider threat program and were the
basis for further investigation.

(7) The frequency that information captured
through the continuous evaluation program or in-
sider threat program was the basis for further inves-
tigation.
(8) Information on any individual whose eligibility for access to classified information was changed as a result of information collected through the continuous evaluation program or insider threat program, including the clearance level of each impacted individual and what position, if any, the individual holds within the agency, number of years the individual has been eligible to access classified information at the level held at the time that the individual was subject to the continuous evaluation program or insider threat program and, if available, the frequency that classified information was accessed by each such individual.

(9) Identification of each database that was accessed.

(10) Protocols for resolution of information captured through the continuous evaluation program or insider threat program that was the basis for further investigation, including the provision of notification to the impacted individual’s supervisor and the impacted individual.

(11) Information on any specific instance in which the continuous evaluation program or insider threat program resulted in the protection of classified information and national security.
(12) Information on the annual and life-cycle costs of the continuous investigation or insider threat program and, in the event that the head of the agency intends to expand the program, information on the anticipated costs of expansion.

(c) PILOT PROGRAM.—The head of any agency that establishes a continuous evaluation program after the date of the enactment of this Act shall be subject to the following requirements:

(1) Before initiating a continuous evaluation program or insider threat program, such head shall conduct a pilot continuous evaluation program or pilot insider threat program that is not shorter than 120 days in duration and uses a representative sample of individuals eligible for access to classified information, including individuals employed by contractors. Participants in the program shall receive notification and, in the event that derogatory information is identified through the program that results in changes to such participant’s eligibility for access to classified information, shall be provided access to the redress process described under section 116.

(2) Before conducting a pilot continuous evaluation program or pilot insider threat program
under paragraph (1), such head shall publish, in the Federal Register, a notice of the program that provides information on the provisions of the program, metrics for evaluating its efficacy, and a privacy impact assessment.

(3) Not later than 90 days after the initiation of a pilot continuous evaluation program or pilot insider threat program pursuant to paragraph (1), such head shall submit to Congress a preliminary report that includes—

(A) the number of individuals evaluated under the program;

(B) the total number of individuals in the agency who are eligible to access classified information;

(C) demographics of the individuals evaluated under the program, including age, race, gender, ethnicity, employer, clearance level, and the number of years the individual has been eligible to access classified information;

(D) a position description for each individual evaluated under the program;

(E) a description of the mechanisms used to conduct the evaluations, including how individuals were selected, whether the evaluations
were randomized, and if so, the nature of the randomization, including the degree to which it was temporally randomized and the degree to which the selection of individuals subject to the program was randomized;

(F) a description of the types of information that were captured through the program and were the basis for further investigation;

(G) the frequency that information captured through the program was the basis for further investigation; and

(H) information on the number of individuals whose eligibility for access to classified information was changed as a result of information collected through the program.

(4) Not later than 180 days after the conclusion of a pilot continuous evaluation program or pilot insider threat program pursuant to paragraph (1) or expansion of a pilot continuous evaluation program or pilot insider threat program, such head shall submit to Congress a final report that updates the information required in the preliminary report under paragraph (3). The report shall include—

(A) an identification of each database that was accessed;
(B) protocols for resolution of information captured through the program that was the basis for further investigation, including the provision of notification to the impacted individual’s supervisor and the impacted individual;

(C) information on any specific instance in which continuous evaluation resulted in the protection of classified information and national security; and

(D) information regarding the annual and life-cycle costs of the program and, in the event that such head intends to expand the program or initiate a continuous evaluation program or insider threat program, information on the anticipated costs of an expansion or initiation.

(5) Prior to expanding a pilot continuous evaluation program or insider threat program or initiating a continuous evaluation program or insider threat program, such head shall secure a privacy impact assessment from the top privacy and civil liberties officials at such agency.

(f) UNCLASSIFIED REPORTS.—All reports required under this section shall be submitted in unclassified form and be made publicly available, but may include a classified annex if necessary.
(g) LIMITATION ON DATA COLLECTION.—Not later than 180 days after the date of enactment of this Act, the head of an agency that operates a continuous evaluation program shall ensure that data collection under the program is limited to databases and other sources of information accessed for a periodic reinvestigation as of the date of enactment of this Act.

(h) DEFINITIONS.—In this section:

(1) CONTINUOUS EVALUATION PROGRAM.—The term “continuous evaluation program” means any program continually reviewing the background of an individual who has been determined to be eligible for access to classified information pursuant to Executive Order 12968 (50 U.S.C. 3161 note) or any other similar authority.

(2) INSIDER THREAT PROGRAM.—The term “insider threat program” means any program monitoring the activity of an individual who has been determined to be eligible for access to classified information to improve insider threat detection and prevention pursuant to Executive Order 13587 (50 U.S.C. 3161 note), or successor order.
SEC. 115. MITIGATING FACTORS IN THE CONTEXT OF A

CONTINUOUS EVALUATION PROGRAM OR INSIDER THREAT PROGRAM.

(a) CONTINUOUS EVALUATION.—Not later than 120 days after the date of enactment of this Act, for each adjudicative guideline for individuals with access to classified information (as described in part 147 of title 32, Code of Federal Regulations or similar successor regulation) the President shall update and tailor the conditions that mitigate security concerns to address continuous evaluation of such individuals performed pursuant to Executive Order 12968 (50 U.S.C. 3161 note) or any other authority, including the implications of recency on the availability of mitigation.

(b) INSIDER THREAT PROGRAM.—Not later than 240 days after the date of enactment of this Act, the President shall establish adjudicative guidelines, including conditions that mitigate security concerns that consider the implications of recency on the availability of mitigation, for an individual who is subject to an adverse decision based on an insider threat program established pursuant to Executive Order 13587 (50 U.S.C. 3161 note) or successor order.
SEC. 116. APPEAL TO THE MERIT SYSTEMS PROTECTION BOARD.

An employee for whom a final determination of ineligibility for a national security position has been made is entitled to appeal to the Merit Systems Protection Board under section 7701 of title 5, United States Code.

SEC. 117. AUTOMATED OR NONGOVERNMENTAL ADJUDICATION PROHIBITED.

(a) In General.—An adjudication by an agency that an individual may not have access to classified information may only be made by a Federal employee and may not be rendered by an automated, electronic, or computer system.

(b) Federal Employee Defined.—In this section, the term “Federal employee” has the meaning given the term “employee” in section 2105 of title 5, United States Code, and includes any member of the uniformed services.

SEC. 118. REPORT ON MEDIA CONTACTS POLICY FOR INTELLIGENCE PERSONNEL.

Not later than 90 days after the date of the enactment of this Act, the head of each element of the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) shall submit to Congress a report on each such element’s implementation of policy directives regarding contacts with news media by intelligence community personnel.
Such report shall describe how each such element’s implementation of such directives protects the free speech rights of intelligence community personnel, including intelligence community personnel who choose to discuss unclassified public policy issues with friends or family members who may use new media technologies.

**TITLE II—DEPARTMENT OF HOMELAND SECURITY CLEARANCE PROCESS REFORMS**

**Subtitle A—Designation**

**SEC. 201. DESIGNATION OF NATIONAL SECURITY SENSITIVE AND PUBLIC TRUST POSITIONS.**

(a) **In General.**—The Secretary of Homeland Security shall require the Department of Homeland Security, including all components of the Department, to designate the sensitivity level of national security positions (pursuant to part 732 of title 5, Code of Federal Regulations, or similar successor regulation) in an accurate and consistent manner within the Department, including all such components.

(b) **Implementation.**—In carrying out subsection (a), the Secretary of Homeland Security shall require the utilization of uniform designation tools throughout the Department of Homeland Security, including all components
of the Department, and provide training to appropriate
staff of the Department, including staff of all such compo-
nents, on such utilization. Such training shall include
guidance on factors for determining eligibility for access
to classified information and facilities with classified infor-
mation.

SEC. 202. AUDITS.

Not later than 180 days after the Director of Na-
tional Intelligence and Director of the Office of Personnel
Management issue a rule for designation of national secu-
rity positions (pursuant to part 732 of title 5, Code of
Federal Regulations, or similar successor regulation), the
Inspector General of the Department of Homeland Secu-
rity shall conduct regular audits of compliance of the De-
partment with such rule.

SEC. 203. REVIEW OF POSITION DESIGNATIONS.

(a) IN GENERAL.—The Secretary of Homeland Secu-

rity, acting through the Chief Security Officer of the De-
partment of Homeland Security, shall biennially conduct
a review of all sensitivity level designations of national se-
curity positions (pursuant to part 732 of title 5, Code of
Federal Regulations, or similar successor regulation) at
the Department.

(b) DETERMINATION.—If during the course of a re-
view required under subsection (a) the Secretary of Home-
land Security determines that a change in the sensitivity level of a position that affects the need for an individual to obtain access to classified information is warranted, such access shall be administratively adjusted or periodic reinvestigation completed, as necessary.

(c) Report.—

(1) In general.—Upon completion of each review required under subsection (a), the Secretary of Homeland Security shall submit to 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 number of positions by classification level and by component of the Department of Homeland Security that are to be redesignated in accordance with subsection (b) to—

(A) require access to classified information;

(B) no longer require access to classified information; or

(C) otherwise require a different level of access to classified information.

(2) Form.—The report required under paragraph (1) shall be submitted in unclassified form and be made publicly available, but may include a
classified annex for any sensitive or classified infor-
mation if necessary.

**Subtitle B—Investigation**

**SEC. 211. INVESTIGATION SERVICES PROVIDER PERFORMANCE.**

(a) **In General.**—The Secretary of Homeland Secu-
rity, acting through the Chief Security Officer of the De-

partment of Homeland Security, shall annually survey the

head of each component or office of the Department with

the authority to adjudicate a current investigation file for

a national security position to help determine whether—

(1) investigation service providers are adhering

to Federal requirements, including requirements

under the Intelligence Reform and Terrorism Pre-

vention Act of 2004 (Public Law 108–458) and re-

quirements promulgated by the Office of Personnel

Management; and

(2) records provided are adequate to conduct

adjudications.

(b) **Contents.**—Each survey under subsection (a)

shall consider the following:

(1) Punctuality of completed personnel security

investigations, including adherence to timelines re-

quired under section 3001 of the Intelligence Reform

(2) Frequency that the adjudicator must seek clarifying or additional information from the investigation service provider.

(3) Frequency that the adjudicator orders a full or partial reinvestigation.

(4) Frequency that the adjudicator finds adverse information after the completed background investigation is submitted by the investigation service provider.

(5) Frequency that the complete investigation file, including investigative notes, is provided.

(6) Overall performance of the investigation service provider.

(7) Satisfaction with the overall performance of the investigation service provider.

(c) Corrective Action.—If information provided under subsection (a) identifies a pattern of performance problems with a particular investigation service provider, the Chief Security Officer of the Department of Homeland Security shall make a recommendation to the Secretary of Homeland Security and, where appropriate, to the head of each component or office of the Department that uses the particular investigation service provider regarding cor-
rective action, including suspension or cancellation of services.

(d) AVAILABILITY.—The Secretary of Homeland Security shall publish the results of each survey under subsection (a) and make each such publication publicly available on the website of the Department of Homeland Security.

SEC. 212. METRICS.
The Secretary of Homeland Security shall utilize metrics, including, to the extent practicable, any metrics in use by the Office of Personnel Management as of the date of the enactment of this Act, to assess the timeliness, completeness, and overall quality of the provision of investigative services by investigation service providers.

Subtitle C—Adjudication

SEC. 221. UNIFORM ADJUDICATION STANDARDS.

(a) IN GENERAL.—The Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall issue uniform adjudication standards, consistent with part 147 of title 32, Code of Federal Regulations, or similar successor regulation, to be utilized by Department adjudicators with respect to adjudicating the eligibility of an individual for access to classified information.
(b) Certification.—Not later than one year after the issuance of the uniform adjudication standards under subsection (a), the Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall require the head of each component and office of the Department with the authority to adjudicate access to classified information of an individual to certify compliance with the uniform adjudication standards under subsection (a).

(c) Audit.—Not later than two years after the last head of a component of the Department of Homeland Security certifies compliance under subsection (b) with the uniform adjudication standards under subsection (a), the Inspector General of the Department shall audit all such components to verify such compliance.

Subtitle D—Denial, Suspension, Revocation, and Appeal

SEC. 231. UNIFORM REVOCATION CRITERIA AND PROCEDURES.

(a) In General.—The Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall issue a Department-wide directive that sets forth uniform criteria and procedures, consistent with any appropriate Federal Governmentwide standards, including notice requirements, for
the suspension, denial, and revocation of eligibility for access to classified information of an individual issued by the Department.

(b) Certification.—Not later than one year after issuance of the uniform criteria and procedures under subsection (a), the Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall require the head of each component and office of the Department with the authority to adjudicate eligibility for access to classified information of an individual to certify compliance with such uniform criteria and procedures.

SEC. 232. ANNUAL REPORTING.

(a) In General.—The Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall annually submit to 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 following:

(1) The number of denials, suspensions, revocations, and appeals of the eligibility for access to classified information of an individual throughout the Department.
(2) The date and status or disposition of each reported action under paragraph (1).

(3) The identification of the originator, whether by a component or headquarters, of each adverse action under paragraph (1), and description of the grounds for each such action.

(4) Demographic data, including data relating to race, sex, national origin, and disability, of each individual for whom eligibility for access to classified information was denied, suspended, revoked, or appealed, and the number of years that each such individual was eligible for access to such information.

(5) In the case of a suspension in excess of 180 days, an explanation for the such timeframe.

(b) FORM.—The report required under subsection (a) shall be submitted in unclassified form and be made publicly available, but may include a classified annex for any sensitive or classified information if necessary.

SEC. 233. FINAL APPEALS PANEL.

(a) IN GENERAL.—The Secretary of Homeland Security shall establish an internal appeals 5-person panel for final national security clearance denial and revocation determinations that is comprised of designees who are career, supervisory employees from departmental components and headquarters.
(b) CHAIR.—The Chief Security Officer of the Department of Homeland Security shall serve as the chair of the panel established pursuant to subsection (a).

(c) POSITIONS.—At least two of the positions on the panel shall be held by non-security related supervisory employees for not more than two consecutive years, and at least one position shall be held by a security related supervisory employee for not more than three consecutive years.

(d) SUB PANELS.—

(1) IN GENERAL.—For each matter before the panel, a 3-person subpanel shall be convened by the chair, and may include the chairman.

(2) PROHIBITION.—The chair may not select a panelist to serve on a 3-person subpanel referred to in paragraph (1) from the same component or office of the Department of Homeland Security as from which the matter before such subpanel originated or who has a prior relationship with any of the individuals involved in such matter.

(e) PROCEDURES.—

(1) IN GENERAL.—Each individual issued access to classified information by the Department of Homeland Security whose access is denied or revoked after a decision from a first-line deciding authority and a supervisor of such first-line deciding
authority may appeal, in writing, to the 5-person ap-
peals panel and appear, with a representative, before
such panel to make a statement.

(2) RULINGS.—A simple majority of the ap-
peals panel is required to uphold or overturn a de-
nial or revocation.

(3) TIMING.—All determinations of the appeals
panel shall be rendered within 90 days of receipt of
an appeal under this section.

(4) FINALITY.—All determinations of the ap-
peals panel shall be final, and no further administra-
tive review shall be permitted.

Subtitle E—Miscellaneous
Provisions

SEC. 241. INTELLIGENCE REFORM AND TERRORISM PRE-
VENTION ACT OF 2004 REVIEW AND SECURITY
CLEARANCE RECIPROCITY.

(a) IN GENERAL.—Not later than two years after the
date of the enactment of this Act, the Comptroller General
of the United States shall submit to 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—

(1) the impact of the implementation of section
3001 of the Intelligence Reform and Terrorism Pre-
vention Act of 2004 (50 U.S.C. 3341; Public Law 108–458) on security clearance processes, including—

(A) with respect to the quality of personnel security investigations and adjudications; and

(B) the extent to which the timelines specified in such section have impacted security clearance backlogs, and include recommendations for areas for reform; and

(2) the extent to which individuals with eligibility for access to classified information, adjudicated by the Secretary of Homeland Security or the head of a component or office of the Department of Homeland Security, are granted reciprocity within the Department and by other agencies, in accordance with subsection (d) of section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341; Public Law 108–458), including—

(A) the extent to which the lack of harmonization of suitability standards is a barrier to such reciprocity; and

(B) recommendations on whether such standards should be included in interagency reciprocity agreements.
(b) FORM.—The report required under subsection (a) shall be submitted in unclassified form and be made publicly available, but may include a classified annex for any sensitive or classified information if necessary.

SEC. 242. OFFICE OF INSPECTOR GENERAL REPORT.

Not later than two years after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall submit to 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 implementation of responsibilities and mandates of the Department under this Act, and the amendments made by this Act. The report required under this section shall be submitted in unclassified form and be made publicly available, but may include a classified annex for any sensitive or classified information if necessary.

SEC. 243. PENALTIES FOR FALSIFICATION RELATING TO AN INVESTIGATION FILE.

Section 1001(a) of title 18, United States Code, is amended by inserting at the end the following: “If the offense involves an investigation file for a national security position (as such term is defined in section 732.102 of title 5, Code of Federal Regulations, or similar successor regulation), then the maximum term of imprisonment oth-
erwise authorized under this section may be increased by one year.”.