H. R. 553

One Hundred Eleventh Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Tuesday, the fifth day of January, two thousand and ten

An Act

To require the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Reducing Over-Classification Act".

SEC. 2. FINDINGS.

Congress finds the following:

(1) The National Commission on Terrorist Attacks Upon the United States (commonly known as the "9/11 Commission") concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies.

(2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.

(3) Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector.

(4) Over-classification of information is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

(5) Federal departments or agencies authorized to make original classification decisions or that perform derivative classification of information are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of classification markings and the policies of the National Archives and Records Administration.

SEC. 3. DEFINITIONS.

In this Act:

(1) DERIVATIVE CLASSIFICATION AND ORIGINAL CLASSIFICATION.—The terms "derivative classification" and "original classification" have the meanings given those terms in Executive Order No. 13526.

(2) EXECUTIVE AGENCY.—The term "Executive agency" has the meaning given that term in section 105 of title 5, United States Code.

(3) EXECUTIVE ORDER NO. 13526.—The term "Executive Order No. 13526" means Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) or any subsequent corresponding executive order.

SEC. 4. CLASSIFIED INFORMATION ADVISORY OFFICER.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

"SEC. 210F. CLASSIFIED INFORMATION ADVISORY OFFICER.

"(a) REQUIREMENT TO ESTABLISH.—The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

"(b) RESPONSIBILITIES.—The responsibilities of the Classified Information Advisory Officer shall be as follows:

"(1) To develop and disseminate educational materials and to develop and administer training programs to assist State, local, and tribal governments (including State, local, and tribal law enforcement agencies) and private sector entities—

"(A) in developing plans and policies to respond to requests related to classified information without communicating such information to individuals who lack appropriate security clearances;

"(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

"(C) on the means by which such personnel may apply for security clearances.

"(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with such personnel, as appropriate.

"(c) INITIAL DESIGNATION.—Not later than 90 days after the date of the enactment of the Reducing Over-Classification Act, the Secretary shall—

"(1) designate the initial Classified Information Advisory Officer; and

"(2) submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a written notification of the designation.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by inserting after the item relating to section 210E the following:

"Sec. 210F. Classified Information Advisory Officer.".

SEC. 5. INTELLIGENCE INFORMATION SHARING.

(a) DEVELOPMENT OF GUIDANCE FOR INTELLIGENCE PRODUCTS.—Paragraph (1) of section 102A(g) of the National Security Act of 1947 (50 U.S.C. 403–1(g)) is amended—

(1) in subparagraph (E), by striking "and" at the end;

(2) in subparagraph (F), by striking the period at the end and inserting a semicolon and "and"; and

(3) by adding at the end the following:

"(G) in accordance with Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) (or any subsequent corresponding executive order), and part 2001 of title 32, Code of Federal Regulations (or any subsequent corresponding regulation), establish—

"(i) guidance to standardize, in appropriate cases, the formats for classified and unclassified intelligence products created by elements of the intelligence community for purposes of promoting the sharing of intelligence products; and

"(ii) policies and procedures requiring the increased use, in appropriate cases, and including portion markings, of the classification of portions of information within one intelligence product.".

(b) CREATION OF UNCLASSIFIED INTELLIGENCE PRODUCTS AS APPROPRIATE FOR STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR STAKEHOLDERS.—

(1) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS AND INFRASTRUCTURE PROTECTION.—Paragraph (3) of section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is amended to read as follows:

"(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

"(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal Government, State, and local government agencies and authorities, the private sector, and other entities; and

"(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.".

(2) ITACG DETAIL.—Section 210D(d) of the Homeland Security Act of 2002 (6 U.S.C. 124k(d)) is amended—

(A) in paragraph (5)—

(i) in subparagraph (D), by striking "and" at the end;

(ii) by redesignating subparagraph (E) as subparagraph (F); and

(iii) by inserting after subparagraph (D) the following:

"(E) make recommendations, as appropriate, to the Secretary or the Secretary's designee, for the further dissemination of intelligence products that could likely

inform or improve the security of a State, local, or tribal government, (including a State, local, or tribal law enforcement agency) or a private sector entity; and";

(B) in paragraph (6)(C), by striking "and" at the end;

(C) in paragraph (7), by striking the period at the end and inserting a semicolon and "and"; and

(D) by adding at the end the following:

"(8) compile an annual assessment of the ITACG Detail's performance, including summaries of customer feedback, in preparing, disseminating, and requesting the dissemination of intelligence products intended for State, local and tribal government (including State, local, and tribal law enforcement agencies) and private sector entities; and

"(9) provide the assessment developed pursuant to paragraph (8) to the program manager for use in the annual reports required by subsection (c)(2).".

(c) INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP ANNUAL REPORT MODIFICATION.—Subsection (c) of section 210D of the Homeland Security Act of 2002 (6 U.S.C. 124k) is amended—

(1) in the matter preceding paragraph (1), by striking ", in consultation with the Information Sharing Council,";

(2) in paragraph (1), by striking "and" at the end;

(3) in paragraph (2), by striking the period at the end and inserting a semicolon and "and"; and

(4) by adding at the end the following:

"(3) in each report required by paragraph (2) submitted after the date of the enactment of the Reducing Over-Classification Act, include an assessment of whether the detailees under subsection (d)(5) have appropriate access to all relevant information, as required by subsection (g)(2)(C).".

SEC. 6. PROMOTION OF ACCURATE CLASSIFICATION OF INFORMATION.

(a) INCENTIVES FOR ACCURATE CLASSIFICATIONS.—In making cash awards under chapter 45 of title 5, United States Code, the President or the head of an Executive agency with an officer or employee who is authorized to make original classification decisions or derivative classification decisions may consider such officer's or employee's consistent and proper classification of information.

(b) INSPECTOR GENERAL EVALUATIONS.—

(1) REQUIREMENT FOR EVALUATIONS.—Not later than September 30, 2016, the inspector general of each department or agency of the United States with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office, shall carry out no less than two evaluations of that department or agency or a component of the department or agency—

(A) to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and

(B) to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency or component.

(2) DEADLINES FOR EVALUATIONS.—

(A) INITIAL EVALUATIONS.—Each first evaluation required by paragraph (1) shall be completed no later than September 30, 2013.

(B) SECOND EVALUATIONS.—Each second evaluation required by paragraph (1) shall review progress made pursuant to the results of the first evaluation and shall be completed no later than September 30, 2016.

(3) REPORTS.—

(A) REQUIREMENT.—Each inspector general who is required to carry out an evaluation under paragraph (1) shall submit to the appropriate entities a report on each such evaluation.

(B) CONTENT.—Each report submitted under subparagraph (A) shall include a description of—

(i) the policies, procedures, rules, regulations, or management practices, if any, identified by the inspector general under paragraph (1)(B); and

(ii) the recommendations, if any, of the inspector general to address any such identified policies, procedures, rules, regulations, or management practices.

(C) COORDINATION.—The inspectors general who are required to carry out evaluations under paragraph (1) shall coordinate with each other and with the Information Security Oversight Office to ensure that evaluations follow a consistent methodology, as appropriate, that allows for cross-agency comparisons.

(4) APPROPRIATE ENTITIES DEFINED.—In this subsection, the term "appropriate entities" means—

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

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

(C) any other committee of Congress with jurisdiction over a department or agency referred to in paragraph (1);

(D) the head of a department or agency referred to in paragraph (1); and

(E) the Director of the Information Security Oversight Office.

SEC. 7. CLASSIFICATION TRAINING PROGRAM.

(a) IN GENERAL.—The head of each Executive agency, in accordance with Executive Order 13526, shall require annual training for each employee who has original classification authority. For employees who perform derivative classification, or are responsible for analysis, dissemination, preparation, production, receipt, publication, or otherwise communication of classified information, training shall be provided at least every two years. Such training shall—

(1) educate the employee, as appropriate, regarding—

(A) the guidance established under subparagraph (G) of section 102A(g)(1) of the National Security Act of 1947 (50 U.S.C. 403–1(g)(1)), as added by section 5(a)(3), regarding the formatting of finished intelligence products;

(B) the proper use of classification markings, including portion markings that indicate the classification of portions of information; and

(C) any incentives and penalties related to the proper classification of intelligence information; and

(2) ensure such training is a prerequisite, once completed successfully, as evidenced by an appropriate certificate or other record, for—

(A) obtaining original classification authority or derivatively classifying information; and

(B) maintaining such authority.

(b) RELATIONSHIP TO OTHER PROGRAMS.—The head of each Executive agency shall ensure that the training required by subsection (a) is conducted efficiently and in conjunction with any other required security, intelligence, or other training programs to reduce the costs and administrative burdens associated with carrying out the training required by subsection (a).

Speaker of the House of Representatives.

Vice President of the United States and
President of the Senate.