Calendar No. 413

111TH CONGRESS *2d Session*	SENATE	REPORT 111–200

REDUCING OVER-CLASSIFICATION ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

H.R. 553

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

MAY 27 (legislative day, MAY 26), 2010.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
89–010 WASHINGTON : 2010

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
ROLAND W. BURRIS, Illinois
EDWARD E. KAUFMAN, Delaware

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
SCOTT P. BROWN, Massachusetts
JOHN MCCAIN, Arizona
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada
LINDSEY GRAHAM, South Carolina

MICHAEL L. ALEXANDER, *Staff Director*
KEVIN J. LANDY, *Chief Counsel*
CHRISTIAN J. BECKNER, *Professional Staff Member*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
JOHN K. GRANT, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

Calendar No. 413

111TH CONGRESS *2d Session* | SENATE | REPORT 111–200

REDUCING OVER-CLASSIFICATION ACT

MAY 27 (legislative day, MAY 26), 2010.—Ordered to be printed

Mr. LIEBERMAN, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany H.R. 553]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (H.R. 553) 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, having considered the same, reports favorably thereon with an amendment and recommends that the bill do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of H.R. 553, as amended by the Committee, is to prevent federal departments and agencies from unnecessarily classifying information or classifying information at a higher and more restricted level than is warranted, and by doing so to promote information sharing across departments and agencies and with State, local, tribal and private sector counterparts, as appropriate.

II. Background and Need for Legislation

U.S. government policies and procedures related to classification are intended to protect information, the unauthorized disclosure of which could cause damage to the national security of the United States. These policies and procedures have been prescribed primarily by a series of Executive Orders, beginning with E.O. 8381, issued in 1940, and updated most recently with E.O. 13526, issued in December 2009. E.O. 13526 and its predecessors describe the types of information that should be classified, establish procedures for access to classified information, and provide guidelines and requirements for the implementation of classification systems, including declassification procedures.

The classification system that developed during the Cold War was focused primarily on protecting sensitive information from the Soviet Union and other traditional nation-state adversaries. But since the fall of the Berlin Wall in 1989, threats to U.S. national security have increasingly come from non-state actors, including terrorist groups, organized criminal networks, and drug trafficking organizations.

Efforts to counter Cold War nation-state threats were handled primarily by the U.S. military and by federal Departments and agencies responsible for diplomacy, intelligence, and law enforcement. Efforts to counter post-Cold War threats involve a broader group of participants, including State, local and tribal governments and law enforcement agencies, as well as private sector entities.

The changing threats to U.S. national security have required our nation's current classification system to take into account factors unknown to its Cold War predecessors. Without doubt, the primary consideration for those making classification decisions must remain whether unauthorized disclosure would damage national security, consistent with the framework established in E.O. 13526 and prior executive orders. But decisions also need to factor in the potential benefits to national security that could result from sharing particular information with the broader group of participants in the national security system. In other words, today's classifiers must weigh not only the harm flowing from unauthorized disclosure, but also the detriment caused by denying critical non-federal actors access to information that could assist their efforts to combat terrorism and other non-state national security threats.

Today's classification system, however, provides insufficient guidance and support to individuals who are making classification decisions, and often leads them to err on the side of over-classifying information. This Act is intended to create a framework by which individuals within the Executive Branch can make more balanced and informed classification decisions, in a way that will strengthen efforts by the United States to address both state-based and non-state threats to national security.

Over-classification of information is particularly problematic with respect to the threat of terrorist attacks against the United States. In its examination of the terrorist attacks of September 11, 2001, the 9/11 Commission found that existing classification policies and procedures nurtured over-classification and excessive compartmentalization of information among agencies in several respects: (1) Each agency's incentive structure opposed sharing, with clear risks

but few rewards for information sharing; (2) no agencies had to pay the substantial long-term costs of over-classifying information; (3) there were no punishments for not sharing information; and (4) agencies cultivated a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.[1]

Recent terrorist plots and attacks against the United States have highlighted the important role of state, local and tribal law enforcement agencies, as well as entities in the private sector, in detecting, preventing and responding to terrorist attacks. In 2005, for example, police officers in Torrance, California investigating a string of gas station robberies uncovered a terrorist plot to attack military facilities and synagogues in southern California. In 2007, a plot to attack Fort Dix in New Jersey was disrupted in part due to an electronics store employee who contacted local police about a suspicious videotape that one of the conspirators had taken to the store to get converted to DVD format.

The current classification system, however, limits the federal government's ability to share information about potential threats with state, local and tribal governments and law enforcement agencies, and with the private sector. Very few officials in state, local and tribal governments and law enforcement agencies have security clearances, and as a result, they often face significant limits to their ability to work as partners with the federal government in terrorism prevention efforts and to receive information about threats that enable them to better protect their communities from the threat of terrorist attacks. In testimony before the House Committee on Homeland Security in 2007, numerous state and local government officials and senior law enforcement officers spoke of the ways in which the classification system inhibited their ability to work in partnership with the federal government on homeland security and terrorism prevention activities.[2]

LEGISLATION PASSED BY THE HOUSE OF REPRESENTATIVES AND SENATE ACTION

The concerns articulated in these House Committee on Homeland Security hearings led Representative Jane Harman, with 13 cosponsors, to introduce the Reducing Over-Classification Act, first in the 110th Congress and then again this Congress. The House bill—H.R. 553 this Congress—focused on reducing the over-classification of information at the Department of Homeland Security (DHS) and enhancing understanding of the classification system by State, local, tribal and private sector entities by establishing an over-classification prevention program at DHS.

As amended by this Committee, H.R. 553 would have a broader scope. It would address the issue of over-classification on a government-wide basis, recognizing that the Department of Homeland Security makes only a very small percentage of original classification decisions each year. The bill would apply many of the House's provisions government-wide and would strengthen the responsibilities

[1] Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, Page 417. 2004.

[2] See House Committee on Homeland Security print of hearings on Over-classification and Pseudo-Classification. Available at *http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg11035279/pdf/CHRG-110hhrg11035279.pdf.*

of the Director of National Intelligence with respect to information sharing. It would strengthen the process whereby the Interagency Threat Assessment Coordination Group can request that intelligence reports be produced at a lower level of classification. And it would establish new government-wide employee incentives, oversight provisions, and training requirements.

The Committee wishes to emphasize that none of the provisions in this Act is intended to supplant the Executive Branch's longstanding authority to determine what information should be appropriately classified within the framework established in Executive Order 13526 and its predecessors.[3] Indeed, the Committee believes that the provisions of the Act complement and do not conflict with Executive Order 13526, and that both the Order and the Act will promote the goals of increased transparency, information sharing, and security. H.R. 553 is merely intended to ensure that this existing framework appropriately considers the information requirements of entities that are playing a critical role in the nation's efforts to combat terrorism and address other non-traditional threats to national security.

III. Legislative History

In the 110th Congress, the House of Representatives passed H.R. 4806, sponsored by Representative Jane Harman and thirteen cosponsors, by voice vote. Representative Harman reintroduced the bill in the 111th Congress, on January 15, 2009, as H.R. 553. The House passed the bill by a voice vote on February 3, 2009. The bill was received in the Senate on February 4, 2009, and referred to the Homeland Security and Governmental Affairs Committee.

The Committee considered the bill on November 4, 2009. Chairman Lieberman and Ranking Minority Member Collins offered an amendment in the nature of the substitute, which made significant changes to the bill by adding new provisions to expand the bill's scope to cover all executive branch agencies, not just at the Department of Homeland Security, by strengthening the responsibilities of the Director of National Intelligence with respect to information sharing; by strengthening the process whereby the Interagency Threat Assessment Coordination Group can request that intelligence reports be produced at a lower level of classification; and by establishing new government-wide employee incentives, oversight provisions, and training requirements.

The Committee adopted the substitute and then voted to report the bill, as amended, both by voice vote. Senators Lieberman, Levin, Akaka, Carper, Pryor, Landrieu, Burris, Collins, and Bennett were present for both votes.

IV. Section-by-Section Analysis of the Legislation

Section 1. Short title

This section states that that this measure may be cited as the "Reducing Over-Classification Act."

[3] The Committee believes that Executive Order 13526 meets the definition of a "subsequent corresponding executive order" to Executive Order 12958 (as modified by Executive Order 13292) as defined in the Act.

Section 2. Findings

This section outlines a series of Congressional findings, including: (1) The 9/11 Commission concluded that there is a need to prevent over-classification of information by the Federal Government; (2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing; (3) Over-classification of information causes considerable confusion about 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 the private sector; and (4) Excessive government secrecy stands in the way of a safer and more secure homeland.

Section 3. Classified Information Advisory Officer

This section modifies subsection (d) of section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) to designate a Classified Information Advisory Officer in the Department of Homeland Security to assist State, local, tribal, and private sector entities that have responsibility for the security of critical infrastructure, in matters related to classified materials. This Officer will be responsible for developing and disseminating training programs and materials to educate these entities on procedures for challenging improper classification and applying for security clearances. This Officer will also assist State, local and tribal entities with developing plans and policies for the use of classified information, including ways to communicate those plans and policies to non-cleared personnel without disclosing classified information. The Officer will also advise the Department of Homeland Security's Under Secretary for Intelligence and Analysis on policies and procedures to facilitate information sharing. The Committee intends that this Officer would serve as both a valuable resource for information and an advocate for these non-federal entities. This office is not intended to process or facilitate individual security clearance applications.

Section 3 of the Act includes references to "State, local, tribal and private sector entities with responsibility [or "that have responsibility"] related to the security of critical infrastructure." In these sections, the language "responsibility related to the security of critical infrastructure" is only intended to modify the term "private sector entity" (or entities) and does not modify State, local or tribal entities.

Section 4. Promotion of appropriate access to information

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 established a Director of National Intelligence (DNI) charged with, among other duties, breaking down barriers to information sharing. IRTPA provides the DNI with access to all national intelligence.[4] This section modifies subsection (b) of section 102A of the National Security Act of 1947 (50 U.S.C. 403–1) to reinforce the authority of the Director of National Intelligence to have maximum access to all information within the intelligence community, including intelligence reports and operational data,

[4] 50 U.S.C. § 403–1(b).

and require that the DNI then ensure maximum access to all such information, consistent with the protection of intelligence sources and methods, to appropriately-cleared individuals in federal, State, local and tribal governments. It also requires that the DNI establish a mechanism to provide individuals from such entities with access to this information (for example, through the establishment or enhancement of information technology systems and networks). This mechanism is not intended to supplant the existing classification challenge procedures but rather to provide an alternative to the challenge process when it has been exhausted or when exigent circumstances require swift action.

Section 5. Intelligence information sharing

This section of the Act includes three distinct provisions intended to improve the sharing of intelligence information with State, local and tribal governments and law enforcement agencies.

a. Standardized formats for intelligence products

This provision modifies paragraph (1) of section 102A(g) of the National Security Act of 1947 (50 U.S.C. 4031(g)) to require the Director of National Intelligence to establish guidance to standardize formats for classified and unclassified finished intelligence products created by elements of the intelligence community for purposes of promoting the sharing of intelligence products.

The formatting of intelligence products can vary depending on which entity within the Intelligence Community created it. Variations in formatting can make it difficult for intelligence products to be easily entered into electronic databases and therefore sorted, searched, and electronically disseminated. The Act requires the DNI to develop guidance to standardize the formats for intelligence products in order to better facilitate information sharing.

b. Portion marking of intelligence products

This provision also directs the DNI to promulgate guidance to require the increased use of portion markings, by which individual sections of a product are marked with their classification level, allowing them to be easily redacted when necessary and thereby allowing sections of the product to be disseminated at a lower classification level when appropriate. It seeks to address a common situation in which intelligence products that contain unclassified information as well as information classified at varied levels end up classified at the highest level, unnecessarily restricting less sensitive information within it to broader audiences for whom such information could be useful.

c. Interagency Threat Assessment and Coordination Group dissemination process

This section gives a new role to the Interagency Threat Assessment and Coordination Group (ITACG), an entity created by Congress in 2007. The ITACG, which is housed at the National Counterterrorism Center, is composed of state, local, and tribal law enforcement and homeland security officers detailed to the group for

the purpose of "integrating, analyzing, and assisting in the dissemination of federally-coordinated information."[5]

Section 5 of the bill requires the head of each federal Department or agency with classification authority, or his or her designee, to share an intelligence product with ITACG if he or she determines that it could benefit a state, local, or tribal government, law enforcement agency, or private sector entity. The ITACG can then recommend that the DHS Undersecretary for Intelligence and Analysis produce a product at the lowest possible classification level that can be provided to appropriate entities. The Committee believes that the ITACG can thus use its understanding of the needs of State, local, and tribal first responders to help direct useful intelligence into the hands of those who most need it. The Under Secretary retains the authority to determine whether or not a useful product can be produced at a lower classification level without risking the disclosure of sources and methods or other sensitive information.

The section also directs the ITACG to report to Congressional committees on the intelligence products shared by the heads of each federal Department or agency with classification authority that could benefit State, local and tribal law enforcement. The report must describe each recommendation made to the ITACG, each recommendation carried out by the Under Secretary of Intelligence and Analysis and each recommendation not carried out.

Section 6. Promotion of accurate classification of intelligence

The section directs Departments and agencies, when making personnel decisions, to consider whether employees are classifying information properly. In his responses to questions from the Senate Select Committee on Intelligence, Admiral Dennis Blair, thennominee for the position of Director of National Intelligence, noted that "there are many penalties for those who disclose classified information and few rewards for those who take the additional effort to write at lower levels of classification."[6] In an effort to counterbalance the apparent incentives to over-classify information, the Act requires that the consistent and proper classification of information be a consideration in awarding personnel incentives.

The section also requires Inspectors General each year through 2014 to assess whether their agencies are appropriately following and administering applicable classification policies, procedures, rules, and regulations. This provision is intended to supplement, not supplant, the National Archives and Records Administration's (NARA's) role as the lead agency for the oversight of the security classification process.

The Committee recognizes the substantial workload already shouldered by the Inspectors General and emphasizes that these evaluations do not necessarily need to examine entire departments and agencies but can be spot-checks of particular offices or components with classification authorities.

---

[5] Section 521 of the Implementing the Recommendations of the 9/11 Commission Act, Public Law 110–53.

[6] Responses of Admiral Dennis C. Blair to Additional Prehearing Questions, p. 54. January 2009. Available at *http://intelligence.senate.gov/090122/blairresponses.pdf.*

Section 7. Classification training program

This section requires annual training for each employee or contractor who has classification authority or is responsible for analysis, dissemination, preparation, production, receiving, publishing or otherwise communicating written classified information. It requires that this training instruct on the proper use of classification markings, including portion marking. This section makes this training a prerequisite for obtaining and renewing classification authority. The Committee expects that, to the greatest extent possible, this new training will be integrated into existing classification training or other appropriate and pre-existing programs.

V. Regulatory Impact and Evaluation

Pursuant to the requirement of paragraph 11(b)(1) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill. CBO states that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, March 26, 2010.

Hon. Joseph I. Lieberman,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 553, the Reducing Over-Classification Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

Douglas W. Elmendorf,
Director.

Enclosure.

H.R. 553—Reducing Over-Classification Act

Summary: H.R. 553 would make several changes to current law designed to promote the sharing of homeland security information with state, local, tribal, and private-sector entities. CBO estimates that implementing the bill would cost $22 million over the 2011–2015 period, assuming the appropriation of the estimated amounts.

Enacting this legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures would not apply.

H.R. 553 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 553 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense) and 800 (general government).

	By fiscal year, in millions of dollars—					
	2011	2012	2013	2014	2015	2011–2015
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Classified Information Advisory Officer:						
Estimated Authorization Level	2	2	2	2	2	10
Estimated Outlays	1	2	2	2	2	9
Inspectors General Evaluations:						
Estimated Authorization Level	3	3	3	3	1	13
Estimated Outlays	3	3	3	3	1	13
Total Changes:						
Estimated Authorization Level	5	5	5	5	3	23
Estimated Outlays	4	5	5	5	3	22

Basis of estimate: For this estimate, CBO assumes the legislation will be enacted near the beginning of fiscal year 2011, that the estimated amounts will be provided annually near the start each fiscal year, and that outlays will follow historical patterns for similar and existing programs.

Classified Information Advisory Officer

Section 3 would establish the position of Classified Information Advisory Officer within the Department of Homeland Security (DHS). The new position would be tasked with developing a program to train the personnel of state, local, tribal, and private-sector entities in the appropriate use of classified information. The training program also would cover the procedures that such entities can use to challenge the classification designation of certain information and the means by which their employees may apply for security clearances.

DHS operates a similar outreach program dealing with cyber security. Based on the amounts requested for that program for 2011, CBO estimates that implementing this section would cost $9 million over the 2011–2015 period, assuming appropriation of the necessary amounts.

Inspectors General evaluations

Section 6 of the bill would require that at least annually until December 31, 2014, the inspectors general of those federal departments or agencies of the United States that originate classified information conduct an evaluation of their agencies' implementation of the applicable classification guidelines. According to information from the Information Security Oversight Office, this provision could require up to 50 evaluations annually.

Under Executive Order 13526, signed by the President on December 29, 2009, agencies that originate or handle classified information are required to establish and maintain self-inspection programs. Integrating the requirements of the bill with the programs established pursuant to Executive Order 13526 could help to reduce the costs of complying with the requirements of this provision. However, since this provision also would require that the inspectors general report on each evaluation conducted, implementing it would most likely require additional staff across the federal government. Based on the number of federal entities that originate classified information, and after adjusting for the potential that some inspectors general represent multiple federal entities, CBO estimates that implementing this provision would cost $13 million over the

2011–2015 period, assuming appropriation of the necessary amounts.

Unclassified intelligence products for state, local, and tribal governments

Section 5 would require the Interagency Threat Assessment and Coordination Group (ITACG), when it determines that certain nonfederal entities could benefit from an intelligence product, to recommend that DHS provide a version of that product, classified at the lowest level possible, to such entities. In addition, this section also would require DHS to report annually on the instances in which ITACG recommended the creation of an intelligence product and the DHS response to such recommendation.

Although the bill would create a new mechanism for ITACG to make recommendations to DHS on intelligence products that would benefit nonfederal entities, the ITACG currently works with DHS to produce intelligence products, such as the Roll Call Release, which is distributed to "street level" law enforcement officers. In addition, DHS is currently tasked with providing homeland security and terrorism information to nonfederal entities. For that purpose, DHS has installed the Homeland Secure Data Network—which allows DHS to share classified information with state and local governments—at 33 intelligence fusion centers nationwide. Based on those factors and input from the staff of the Program Manager of the Information Sharing Environment at DHS, CBO estimates that the cost of implementing this provision would not be significant in any year and would be primarily related to the reporting requirements imposed by the bill.

Pay-As-You-Go considerations: None.

Intergovernmental and private-sector impact: H.R. 553 contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimate prepared by: Federal costs: Jason Wheelock; Impact on state, local, and tribal governments: Melissa Merrell; Impact on the private sector: Paige Piper/Bach.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause x(x) of rule XIII of the Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

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

* * * * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Information and Analysis and Infrastructure Protection; Access to Information

SECTION 201. [6 U.S.C. 121] INFORMATION AND ANALYSIS AND INFRASTRUCTURE PROTECTION.

* * * * * * *

(d) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS AND INFRASTRUCTURE PROTECTION.—The responsibilities of the Secretary relating to intelligence and analysis and infrastructure protection shall be as follows:

* * * * * * *

(26) To identify and designate, acting through the Under Secretary for Intelligence and Analysis, a Classified Information Advisory Officer to assist State, local, tribal and private sector entities that have responsibility for the security of critical infrastructure, in matters related to classified materials, as described in Section 210F.

* * * * * * *

SECTION 210D. [6 U.S.C. 124k] INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP.

* * * * * * *

(c) RESPONSIBILITIES OF PROGRAM MANAGER.—The program manager, in consultation with the Information Sharing Council, shall—

(1) monitor and assess the efficacy of the ITACG; [and]

(2) not later than 180 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and at least annually thereafter, submit to the Secretary, the Attorney General, the Director of National Intelligence, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the progress of the ITACG*; and*

(3) in each report required by paragraph (2) submitted after the date of enactment of the Reducing Over-Classification Act, include a description of the progress made by the head of each Federal department and agency to share information with the ITACG pursuant to section 102A(g)(3)(A) of the National Security Act of 1947 (50 U.S.C. 403–1(g)(3)(A)).

* * * * * * *

SECTION 210F. CLASSIFIED INFORMATION ADVISORY OFFICER.

(a) REQUIREMENTS TO ESTABLISH.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, 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, tribal and private sector entities with responsibility related to the security of critical infrastructure—

(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.

* * * * * * *

NATIONAL SECURITY ACT OF 1947

TITLE I—COORDINATION FOR NATIONAL SECURITY

* * * * * * *

SECTION 102A. RESPONSIBILITIES AND AUTHORITIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

* * * * * * *

(b) ACCESS TO INTELLIGENCE.—

(1) Unless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.

(2) The Director of National Intelligence shall—

(A) consistent with paragraph (1), have access to all intelligence information, including intelligence reports, operational data, and other associated information, produced by any element of the intelligence community; and

(B) consistent with the protection of intelligence sources and methods, as determined by the Director—

(i) ensure maximum access to the intelligence information referenced in subparagraph (A) for an employee of a department, agency, or other entity of the Federal

Government or of a State, local or tribal government who has an appropriate security clearance; and

(ii) provide a mechanism within the Office of the Director of National Intelligence for the Director to direct access to the information referenced in subparagraph (A) for an employee referred to in clause (i).

* * * * * * *

(g) INTELLIGENCE INFORMATION SHARING.—

(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

* * * * * * *

(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; **[**and**]**

(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program*; and*

(G) in accordance with Executive Order No. 12958, as amended by Executive Order No. 13292 (68 Fed. Reg. 15315; relating to classification of national security information) (or any subsequent corresponding executive order), and parts 2001 and 2004 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.

(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

(3)(A) If the head of a Federal department or agency determines that an intelligence product which includes homeland security information, as defined in section 892(f) of the Homeland Security Information Sharing Act (6 U.S.C. 482(f)), or terrorism information, as defined in section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(a)), could likely benefit a State, local, or tribal government, a law enforcement agency, or a private sector entity with responsibility for the security of critical infrastructure, such head shall share that intelligence product with the Interagency Threat Assessment and Coordination Group established in Section 210D(a) of the Homeland Security Act of 2002 (6 U.S.C. 124k(a)).

(B) If the Interagency Threat Assessment and Coordination Group determines that an intelligence product referred to in subparagraph (A), or any other intelligence product that such

Group has access to, could likely benefit a State, local or tribal government, a law enforcement agency, or a private sector entity, the Group shall recommend to the Under Secretary for Intelligence and Analysis of the Department of Homeland Security that the Under Secretary produce an intelligence product that is unclassified or that is classified at the lowest possible level—

(i) based on the intelligence product referred to in subparagraph (a), in a manner consistent with the guidance established under paragraph (1)(G)(i); and

(ii) provide such product to the appropriate entity or agency.

(C)(i) The Secretary of Homeland Security shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives an annual report on activities carried out under this paragraph. Each report shall include a description of—

(I) each recommendation made to the Under Secretary for Intelligence and Analysis under subparagraph (B);

(II) each such recommendation that was carried out by the Under Secretary; and

(III) each such recommendation that was not carried out by the Under Secretary.

(ii) The initial report required under clause (i) shall be submitted not later than 270 days after the date of the enactment of the Reducing Over-Classification Act and no reports shall be required under clause (i) after December 31, 2014.

(4) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency shall not be considered to have met any obligation to provide any information, report, assessment or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment or other material to the Director of National Intelligence or the National Counterterrorism Center.

(5) Not later than February 1 of each year, the Director of National Intelligence shall submit to the President and to the Congress an annual report that identifies any statute, regulation, policy or practice that the Director believes impedes the ability of the Director to fully and effectively implement paragraph (1).

* * * * * * *

○