

(1) With respect to an award of a contract that requires a subcontracting plan, a mentor firm may receive evaluation credit for participating in the Program.

(2) With respect to an award of a contract that requires a subcontracting plan, a mentor firm may receive credit for a protégé firm performing as a first tier subcontractor or a subcontractor at any tier in an amount equal to the total dollar value of any subcontracts awarded to such protégé firm.

(3) A protégé firm may receive technical, managerial, financial, or any other mutually agreed upon benefit from a mentor firm, including a subcontract award.

#### (f) Reporting

Not later than one year after December 23, 2022, and annually thereafter, the head of the Office of Small and Disadvantaged Business Utilization shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Homeland Security and the Committee on Small Business of the House of Representatives a report that—

(1) identifies each agreement between a mentor firm and a protégé firm entered into under this section, including the number of protégé firm participants that are—

- (A) small business concerns;
- (B) small business concerns owned and controlled by veterans;
- (C) small business concerns owned and controlled by service-disabled veterans;
- (D) qualified HUBZone small business concerns;
- (E) small business concerns owned and controlled by socially and economically disadvantaged individuals;
- (F) small business concerns owned and controlled by women;
- (G) historically Black colleges and universities; and
- (H) minority-serving institutions;

(2) describes the type of assistance provided by mentor firms to protégé firms;

(3) identifies contracts within the Department in which a mentor firm serving as the prime contractor provided subcontracts to a protégé firm under the Program; and

(4) assesses the degree to which there has been—

- (A) an increase in the technical capabilities of protégé firms; and
- (B) an increase in the quantity and estimated value of prime contract and subcontract awards to protégé firms for the period covered by the report.

#### (g) Rule of construction

Nothing in this section may be construed to limit, diminish, impair, or otherwise affect the authority of the Department to participate in any program carried out by or requiring approval of the Small Business Administration or adopt or follow any regulation or policy that the Administrator of the Small Business Administration may promulgate, except that, to the extent that any provision of this section (includ-

ing subsection (h)) conflicts with any other provision of law, regulation, or policy, this section shall control.

#### (h) Definitions

In this section:

##### (1) Historically Black college or university

The term “historically Black college or university” has the meaning given the term “part B institution” in section 1061 of title 20.

##### (2) Mentor firm

The term “mentor firm” means a for-profit business concern that is not a small business concern that—

- (A) has the ability to assist and commits to assisting a protégé to compete for Federal prime contracts and subcontracts; and
- (B) satisfies any other requirements imposed by the Secretary.

##### (3) Minority-serving institution

The term “minority-serving institution” means an institution of higher education described in section 1067q(a) of title 20.<sup>1</sup>

##### (4) Protégé firm

The term “protégé firm” means a small business concern, a historically Black college or university, or a minority-serving institution that—

- (A) is eligible to enter into a prime contract or subcontract with the Department; and
- (B) satisfies any other requirements imposed by the Secretary.

##### (5) Small Business Act definitions

The terms “small business concern”, “small business concern owned and controlled by veterans”, “small business concern owned and controlled by service-disabled veterans”, “qualified HUBZone small business concern”, “and small<sup>2</sup> business concern owned and controlled by women” have the meanings given such terms, respectively, under section 632 of title 15. The term “small business concern owned and controlled by socially and economically disadvantaged individuals” has the meaning given such term in section 637(d)(3)(C) of title 15.

(Pub. L. 107–296, title VIII, §890D, as added Pub. L. 117–263, div. G, title LXXI, §7115(a), Dec. 23, 2022, 136 Stat. 3633.)

#### Editorial Notes

##### REFERENCES IN TEXT

Section 1067q(a) of title 20, referred to in subsec. (h)(3), was in the original “section 317 of the Higher Education Act of 1965 (20 U.S.C. 1067q(a))” and was translated as reading “section 371(a) of the Higher Education Act of 1965”, to reflect the probable intent of Congress.

#### PART I—INFORMATION SHARING

### § 481. Short title; findings; and sense of Congress

#### (a) Short title

This part may be cited as the “Homeland Security Information Sharing Act”.

<sup>1</sup> See References in Text note below.

<sup>2</sup> So in original. The opening quotation marks preceding “and” probably should precede “small”.

**(b) Findings**

Congress finds the following:

(1) The Federal Government is required by the Constitution to provide for the common defense, which includes terrorist attack.

(2) The Federal Government relies on State and local personnel to protect against terrorist attack.

(3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.

(4) Some homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack.

(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information.

(6) Granting security clearances to certain State and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among Federal, State, and local levels of government.

(7) Methods exist to declassify, redact, or otherwise adapt classified information so it may be shared with State and local personnel without the need for granting additional security clearances.

(8) State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by Federal agencies.

(9) The Federal Government and State and local governments and agencies in other jurisdictions may benefit from such information.

(10) Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.

(11) Information systems, including the National Law Enforcement Telecommunications System and the Terrorist Threat Warning System, have been established for rapid sharing of classified and sensitive but unclassified information among Federal, State, and local entities.

(12) Increased efforts to share homeland security information should avoid duplicating existing information systems.

**(c) Sense of Congress**

It is the sense of Congress that Federal, State, and local entities should share homeland security information to the maximum extent practicable, with special emphasis on hard-to-reach urban and rural communities.

(Pub. L. 107-296, title VIII, § 891, Nov. 25, 2002, 116 Stat. 2252.)

**Editorial Notes****REFERENCES IN TEXT**

This part, referred to in subsec. (a), was in the original “This subtitle”, meaning subtitle I (§§ 891-899) of title VIII of Pub. L. 107-296, Nov. 25, 2002, 116 Stat. 2252,

which enacted this part, amended section 2517 of Title 18, Crimes and Criminal Procedure, Rule 6 of the Federal Rules of Criminal Procedure, set out in the Appendix to Title 18, and sections 1806, 1825, and 3365 of Title 50, War and National Defense, and amended provisions set out as a note under section 2517 of Title 18. For complete classification of subtitle I to the Code, see Tables.

**Statutory Notes and Related Subsidiaries****REPORTS TO CONGRESS**

Pub. L. 110-28, title III, May 25, 2007, 121 Stat. 139, provided in part: “That starting July 1, 2007, the Secretary of Homeland Security shall submit quarterly reports to the Committees on Appropriations of the Senate and the House of Representatives detailing the information required in House Report 110-107.”

**§ 482. Facilitating homeland security information sharing procedures****(a) Procedures for determining extent of sharing of homeland security information**

(1) The President shall prescribe and implement procedures under which relevant Federal agencies—

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

**(b) Procedures for sharing of homeland security information**

(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.

(2) Each information sharing system through which information is shared under paragraph (1) shall—

(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;

(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—

(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.

(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.

**(c) Sharing of classified information and sensitive but unclassified information with State and local personnel**

(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a).

(2) It is the sense of Congress that such procedures may include 1 or more of the following means:

(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.

(B) With respect to information that is sensitive but unclassified, entering into non-disclosure agreements with appropriate State and local personnel.

(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.

(3)(A) The Secretary shall establish a program to provide appropriate training to officials described in subparagraph (B) in order to assist such officials in—

(i) identifying sources of potential terrorist threats through such methods as the Secretary determines appropriate;

(ii) reporting information relating to such potential terrorist threats to the appropriate Federal agencies in the appropriate form and manner;

(iii) assuring that all reported information is systematically submitted to and passed on by the Department for use by appropriate Federal agencies; and

(iv) understanding the mission and roles of the intelligence community to promote more effective information sharing among Federal, State, and local officials and representatives of the private sector to prevent terrorist attacks against the United States.

(B) The officials referred to in subparagraph (A) are officials of State and local government agencies and representatives of private sector entities with responsibilities relating to the oversight and management of first responders, counterterrorism activities, or critical infrastructure.

(C) The Secretary shall consult with the Attorney General to ensure that the training program established in subparagraph (A) does not duplicate the training program established in section 908 of the USA PATRIOT Act (Public Law 107-56; 28 U.S.C. 509 note).

(D) The Secretary shall carry out this paragraph in consultation with the Director of Central Intelligence and the Attorney General.

**(d) Responsible officials**

For each affected Federal agency, the head of such agency shall designate an official to administer this chapter with respect to such agency.

**(e) Federal control of information**

Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.

**(f) Definitions**

As used in this section:

(1) The term “homeland security information” means any information possessed by a Federal, State, or local agency that—

(A) relates to the threat of terrorist activity;

(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;

(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or

(D) would improve the response to a terrorist act.

(2) The term “intelligence community” has the meaning given such term in section 3003(4) of title 50.

(3) The term “State and local personnel” means any of the following persons involved in prevention, preparation, or response for terrorist attack:

(A) State Governors, mayors, and other locally elected officials.

(B) State and local law enforcement personnel and firefighters.

(C) Public health and medical professionals.

(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.

(E) Other appropriate emergency response agency personnel.

(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.

(4) The term “State” includes the District of Columbia and any commonwealth, territory, or possession of the United States.

#### (g) Construction

Nothing in this chapter shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this chapter to receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

(Pub. L. 107–296, title VIII, § 892, Nov. 25, 2002, 116 Stat. 2253; Pub. L. 108–177, title III, § 316(a), Dec. 13, 2003, 117 Stat. 2610.)

#### Editorial Notes

##### REFERENCES IN TEXT

This chapter, referred to in subsecs. (d) and (g), was in the original “this Act”, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

##### AMENDMENTS

2003—Subsec. (c)(3). Pub. L. 108–177 added par. (3).

#### Statutory Notes and Related Subsidiaries

##### CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Cen-

tral Intelligence or the Director of the Central Intelligence Agency in the Director’s capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.

#### Executive Documents

##### EX. ORD. NO. 13311. HOMELAND SECURITY INFORMATION SHARING

Ex. Ord. No. 13311, July 29, 2003, 68 F.R. 45149, as amended by Ex. Ord. No. 13388, § 8(a), Oct. 25, 2005, 70 F.R. 62025, provided:

By the authority vested in me by the Constitution and the laws of the United States, including sections 892 and 893 of the Homeland Security Act of 2002 (the “Act”) (6 U.S.C. 482 and 483) and section 301 of title 3, United States Code, it is hereby ordered as follows:

SECTION 1. *Assignment of Functions.* (a) The functions of the President under section 892 of the Act are assigned to the Secretary of Homeland Security (the “Secretary”), except the functions of the President under subsections 892(a)(2) and 892(b)(7).

(b) Subject to section 2(b) of this order, the function of the President under section 893 of the Act is assigned to the Secretary.

(c) Procedures issued by the Secretary in the performance of the function of the President under section 892(a)(1) of the Act shall apply to all agencies of the Federal Government. Such procedures shall specify that the President may make, or may authorize another officer of the United States to make, exceptions to the procedures.

(d) The function of the President under section 892(b)(7) of the Act is delegated to the Attorney General and the Director of National Intelligence, to be exercised jointly.

(e) In performing the functions assigned to the Secretary by subsection (a) of this section, the Secretary shall coordinate with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Energy, the Director of the Office of Management and Budget, the Director of National Intelligence, the Archivist of the United States, and as the Secretary deems appropriate, other officers of the United States.

(f) A determination, under the procedures issued by the Secretary in the performance of the function of the President under section 892(a)(1) of the Act, as to whether, or to what extent, an individual who falls within the category of “State and local personnel” as defined in sections 892(f)(3) and (f)(4) of the Act shall have access to information classified pursuant to [former] Executive Order 12958 of April 17, 1995, as amended, is a discretionary determination and shall be conclusive and not subject to review or appeal.

SEC. 2. *Rules of Construction.* Nothing in this order shall be construed to impair or otherwise affect:

(a) the authority of the Director of National Intelligence under section 102A(i)(1) of the National Security Act of 1947, as amended (50 U.S.C. 403–3(c)(7) [sic]) [50 U.S.C. 3024(i)(1)], to protect intelligence sources and methods from unauthorized disclosure;

(b) the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals; or

(c) the provisions of Executive Orders 12958 of April 17, 1995 [former 50 U.S.C. 435 note], as amended, and 12968 of August 2, 1995 [50 U.S.C. 3161 note], as amended.

SEC. 3. *General Provision.* This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH.

**§ 483. Report****(a) Report required**

Not later than 12 months after November 25, 2002, the President shall submit to the congressional committees specified in subsection (b) a report on the implementation of section 482 of this title. The report shall include any recommendations for additional measures or appropriation requests, beyond the requirements of section 482 of this title, to increase the effectiveness of sharing of information between and among Federal, State, and local entities.

**(b) Specified congressional committees**

The congressional committees referred to in subsection (a) are the following committees:

- (1) The Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.
- (2) The Select Committee on Intelligence and the Committee on the Judiciary of the Senate.

(Pub. L. 107–296, title VIII, § 893, Nov. 25, 2002, 116 Stat. 2255.)

**Executive Documents****DELEGATION OF FUNCTIONS**

For assignment of function of President under this section, subject to certain limitations, to Secretary of Homeland Security, see Ex. Ord. No. 13311, §1(b), July 29, 2003, 68 F.R. 45149, set out as a note under section 482 of this title.

**§ 484. Authorization of appropriations**

There are authorized to be appropriated such sums as may be necessary to carry out section 482 of this title.

(Pub. L. 107–296, title VIII, § 894, Nov. 25, 2002, 116 Stat. 2256.)

**§ 484a. Reciprocal information sharing**

Acting in accordance with a bilateral or multilateral arrangement, the Secretary, in the Secretary's discretion and on the basis of reciprocity, may provide information from the National Sex Offender Registry relating to a conviction for a sex offense against a minor (as such terms are defined in section 20911 of title 34) to a foreign government upon the request of the foreign government, and may receive comparable information from the foreign government.

(Pub. L. 107–296, title VIII, § 895, as added Pub. L. 117–347, title III, § 323(a)(1)(B), Jan. 5, 2023, 136 Stat. 6207.)

**Editorial Notes****PRIOR PROVISIONS**

A prior section 895 of Pub. L. 107–296 amended Rule 6 of the Federal Rules of Criminal Procedure, set out in the Appendix to Title 18, Crimes and Criminal Procedure, prior to repeal by Pub. L. 117–347, title III, § 323(a)(1)(A), Jan. 5, 2023, 136 Stat. 6206.

**§ 485. Information sharing****(a) Definitions**

In this section:

**(1) Homeland security information**

The term “homeland security information” has the meaning given that term in section 482(f) of this title.

**(2) Information Sharing Council**

The term “Information Sharing Council” means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).

**(3) Information sharing environment**

The terms “information sharing environment” and “ISE” mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.

**(4) Program manager**

The term “program manager” means the program manager designated under subsection (f).

**(5) Terrorism information**

The term “terrorism information”—

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

- (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
- (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
- (iii) communications of or by such groups or individuals; or
- (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information.

**(6) Weapons of mass destruction information**

The term “weapons of mass destruction information” means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

**(b) Information sharing environment****(1) Establishment**

The President shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national

security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

## **(2) Attributes**

The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties;

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;

(J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;

(K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;

(L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;

(M) permits analysts to collaborate both independently and in a group (commonly known as "collective and noncollective collaboration"), and across multiple levels of national security information and controlled unclassified information;

(N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and

(O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

## **(3) Delegation**

### **(A) In general**

Subject to subparagraph (B), the President may delegate responsibility for carrying out this subsection.

### **(B) Limitation**

The President may not delegate responsibility for carrying out this subsection to the Director of National Intelligence.

## **(c) Preliminary report**

Not later than 180 days after December 17, 2004, the program manager shall, in consultation with the Information Sharing Council—

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

## **(d) Guidelines and requirements**

As soon as possible, but in no event later than 270 days after December 17, 2004, the President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42, issue guidelines that—

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

**(e) Implementation plan report**

Not later than one year after December 17, 2004, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with—

(A) the authority of the Director of National Intelligence under this title,<sup>1</sup> and the amendments made by this title,<sup>1</sup> to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Department of Justice, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

**(f) Program manager****(1) Designation**

Not later than 120 days after December 17, 2004, with notification to Congress, the President shall designate an individual as the pro-

gram manager responsible for information sharing across the Federal Government. Beginning on December 20, 2019, each individual designated as the program manager shall be appointed by the Director of National Intelligence. The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

**(2) Duties and responsibilities****(A) In general**

The program manager shall, in consultation with the Information Sharing Council—

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;

(iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;

(iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and

(v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

**(B) Content of policies, procedures, guidelines, rules, and standards**

The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and

<sup>1</sup> See References in Text note below.

agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

**(g) Information Sharing Council**

**(1) Establishment**

There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve until removed from service or replaced by the President (at the sole discretion of the President) with a successor body.

**(2) Specific duties**

In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall—

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles,<sup>2</sup> and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments;

(G) assist the program manager in identifying and resolving information sharing disputes between Federal departments, agencies, and components;

(H) identify appropriate personnel for assignment to the program manager to support staffing needs identified by the program manager; and

(I) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

**(3) Consultation**

In performing its duties, the Information Sharing Council shall consider input from per-

sons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

**(4) Inapplicability of chapter 10 of title 5**

The Information Sharing Council (including any subsidiary group of the Information Sharing Council) shall not be subject to the requirements of chapter 10 of title 5.

**(5) Detailees**

Upon a request by the Director of National Intelligence, the departments and agencies represented on the Information Sharing Council shall detail to the program manager, on a reimbursable basis, appropriate personnel identified under paragraph (2)(H).

**(h) Agency responsibilities**

The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

**(i) Report on the information sharing environment**

**(1) In general**

Not later than 180 days after August 3, 2007, the President shall report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Homeland Security of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives on the feasibility of—

(A) eliminating the use of any marking or process (including “Originator Control”) intended to, or having the effect of, restricting the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, between and among participants in the information sharing environment, unless the President has—

(i) specifically exempted categories of information from such elimination; and

(ii) reported that exemption to the committees of Congress described in the matter preceding this subparagraph; and

(B) continuing to use Federal agency standards in effect on August 3, 2007, for the collection, sharing, and access to information within the scope of the information

<sup>2</sup> So in original. Probably should be “rules.”



sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, relating to citizens and lawful permanent residents;

(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, for a particular purpose that the Federal Government, through an appropriate process established in consultation with the Privacy and Civil Liberties Oversight Board established under section 2000ee of title 42, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an “authorized use” standard); and

(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, in any cases in which—

(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and

(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information.

## (2) Definition

In this subsection, the term “anonymized data” means data in which the individual to whom the data pertains is not identifiable with reasonable efforts, including information that has been encrypted or hidden through the use of other technology.

## (j) Additional positions

The program manager is authorized to hire not more than 40 full-time employees to assist the program manager in—

(1) activities associated with the implementation of the information sharing environment, including—

(A) implementing the requirements under subsection (b)(2); and

(B) any additional implementation initiatives to enhance and expedite the creation of the information sharing environment; and

(2) identifying and resolving information sharing disputes between Federal departments, agencies, and components under subsection (f)(2)(A)(iv).

## (k) Authorization of appropriations

There is authorized to be appropriated to carry out this section \$30,000,000 for each of fiscal years 2008 and 2009.

(Pub. L. 108–458, title I, §1016, Dec. 17, 2004, 118 Stat. 3664; Pub. L. 110–53, title V, §504, Aug. 3, 2007, 121 Stat. 313; Pub. L. 111–259, title VIII, §806(a)(1), Oct. 7, 2010, 124 Stat. 2748; Pub. L. 116–92, div. E, title LXIV, §6402, Dec. 20, 2019, 133 Stat. 2196; Pub. L. 116–260, div. W, title III, §307, Dec. 27, 2020, 134 Stat. 2368; Pub. L. 117–263, div. F, title LXVIII, §6811(c)(1), Dec. 23, 2022, 136 Stat. 3600; Pub. L. 117–286, §4(a)(17), Dec. 27, 2022, 136 Stat. 4307.)

## Editorial Notes

### REFERENCES IN TEXT

Executive Order 13356, referred to in subsec. (a)(2), which was formerly set out as a note below, was revoked by Ex. Ord. No. 13388, set out as a note below, which established an Information Sharing Council consistent with subsec. (g) of this section.

This title, referred to in subsec. (e)(10)(A), is title I of Pub. L. 108–458, Dec. 17, 2004, 118 Stat. 3643, known as the National Security Intelligence Reform Act of 2004. For complete classification of title I to the Code, see Tables.

### CODIFICATION

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as part of the National Security Intelligence Reform Act of 2004, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

### AMENDMENTS

2022—Subsec. (g)(4). Pub. L. 117–286 substituted “chapter 10 of title 5” for “Federal Advisory Committee Act” in heading and “chapter 10 of title 5.” for “the Federal Advisory Committee Act (5 U.S.C. App.)” in text.

Subsecs. (h) to (l). Pub. L. 117–263 redesignated subsecs. (i) to (l) as (h) to (k), respectively, and struck out former subsec. (h) which related to performance management reports.

2020—Subsec. (b)(1). Pub. L. 116–260, §307(1), substituted “President” for “Director of National Intelligence” in introductory provisions.

Subsec. (b)(2). Pub. L. 116–260, §307(2), substituted “President” for “Director of National Intelligence” in two places in introductory provisions.

Subsec. (b)(3). Pub. L. 116–260, §307(3), added par. (3).

2019—Subsec. (b)(1). Pub. L. 116–92, §6402(a)(1), substituted “Director of National Intelligence” for “President” in introductory provisions.

Subsec. (b)(2). Pub. L. 116–92, §6402(a)(2), substituted “Director of National Intelligence” for “President” in two places in introductory provisions.

Subsec. (f)(1). Pub. L. 116–92, §6402(b), substituted “Beginning on December 20, 2019, each individual designated as the program manager shall be appointed by the Director of National Intelligence.” for “The individual designated as the program manager shall serve as program manager until removed from service or replaced by the President (at the President’s sole discretion).”

2010—Subsec. (e)(10)(B). Pub. L. 111–259 substituted “Department of Justice” for “Attorney General”.

2007—Subsec. (a)(1), (2). Pub. L. 110–53, §504(1)(A), (B), added par. (1) and redesignated former par. (1) as (2). Former par. (2) redesignated (3).

Subsec. (a)(3). Pub. L. 110–53, §504(1)(C), added par. (3) and struck out heading and text of former par. (3). Text read as follows: “The terms ‘information sharing environment’ and ‘ISE’ mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.”

Pub. L. 110–53, §504(1)(A), redesignated par. (2) as (3). Former par. (3) redesignated (4).

Subsec. (a)(4). Pub. L. 110–53, §504(1)(A), redesignated par. (3) as (4). Former par. (4) redesignated (5).

Subsec. (a)(5). Pub. L. 110-53, §504(1)(D), added par. (5) and struck out heading and text of former par (5). Text read as follows: “The term ‘terrorism information’ means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

“(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

“(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

“(C) communications of or by such groups or individuals; or

“(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.”

Pub. L. 110-53, §504(1)(A), redesignated par. (4) as (5). Subsec. (a)(6). Pub. L. 110-53, §504(1)(E), added par. (6). Subsec. (b)(2)(J) to (O). Pub. L. 110-53, §504(2), added subpars. (J) to (O).

Subsec. (f)(1). Pub. L. 110-53, §504(3)(A), substituted “until removed from service or replaced” for “during the two-year period beginning on the date of designation under this paragraph unless sooner removed from service and replaced” and “The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law” for “The program manager shall have and exercise governmentwide authority”.

Subsec. (f)(2)(A)(ii) to (v). Pub. L. 110-53, §504(3)(B), added cls. (ii) to (iv), redesignated former cl. (iii) as (v), and struck out former cl. (ii) which read as follows: “assist in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE; and”.

Subsec. (g)(1). Pub. L. 110-53, §504(4)(A), substituted “until removed from service or replaced” for “during the two-year period beginning on the date of the initial designation of the program manager by the President under subsection (f)(1) of this section, unless sooner removed from service and replaced”.

Subsec. (g)(2)(G) to (I). Pub. L. 110-53, §504(4)(B), added subpars. (G) and (H) and redesignated former subpar. (G) as (I).

Subsec. (g)(4). Pub. L. 110-53, §504(4)(C), inserted “(including any subsidiary group of the Information Sharing Council)” before “shall not be subject”.

Subsec. (g)(5). Pub. L. 110-53, §504(4)(D), added par. (5).

Subsec. (h)(1). Pub. L. 110-53, §504(5), substituted “and not later than June 30 of each year thereafter” for “and annually thereafter”.

Subsecs. (j) to (l). Pub. L. 110-53, §504(6), added subsecs. (j) to (l) and struck out heading and text of former subsec. (j). Text read as follows: “There is authorized to be appropriated to carry out this section \$20,000,000 for each of fiscal years 2005 and 2006.”

#### Statutory Notes and Related Subsidiaries

##### EFFECTIVE DATE

For determination by President that section takes effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 3001 of Title 50, War and National Defense.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see sec-

tion 1097(a) of Pub. L. 108-458, set out as an Effective Date of 2004 Amendment; Transition Provisions note under section 3001 of Title 50, War and National Defense.

#### PROCEDURES TO CLEAR INDIVIDUALS FROM TERRORIST DATABASE LISTS

Pub. L. 109-295, title V, §556, Oct. 4, 2006, 120 Stat. 1391, provided that: “Not later than six months after the date of enactment of this Act [Oct. 4, 2006], the Secretary of Homeland Security shall establish revised procedures for expeditiously clearing individuals whose names have been mistakenly placed on a terrorist database list or who have names identical or similar to individuals on a terrorist database list. The Secretary shall advise Congress of the procedures established.”

#### Executive Documents

##### EXECUTIVE ORDER NO. 13356

Ex. Ord. No. 13356, Aug. 27, 2004, 69 F.R. 53599, which provided for strengthening the sharing of terrorism information to protect Americans, was revoked by Ex. Ord. No. 13388, §8(b), Oct. 25, 2005, 70 F.R. 62025, set out below.

##### EX. ORD. NO. 13388. FURTHER STRENGTHENING THE SHARING OF TERRORISM INFORMATION TO PROTECT AMERICANS

Ex. Ord. No. 13388, Oct. 25, 2005, 70 F.R. 62023, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) [6 U.S.C. 485], and in order to further strengthen the effective conduct of United States counterterrorism activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

SECTION 1. *Policy.* To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:

(a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information; and

(b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).

SEC. 2. *Duties of Heads of Agencies Possessing or Acquiring Terrorism Information.* To implement the policy set forth in section 1 of this order, the head of each agency that possesses or acquires terrorism information:

(a) shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency, unless otherwise directed by the President, and consistent with (i) the statutory responsibilities of the agencies providing and receiving the information; (ii) any guidance issued by the Attorney General to fulfill the policy set forth in subsection 1(b) of this order; and (iii) other applicable law, including sections 102A(g) and (i) of the National Security Act of 1947 [50 U.S.C. 3024(g), (i)], section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 [6 U.S.C. 485] (including any policies, procedures, guidelines, rules, and standards issued pursuant thereto), sections 202 and 892 of the Homeland Security Act of 2002 [6 U.S.C. 122, 482], [former] Executive Order

12958 of April 17, 1995, as amended, and Executive Order 13311 of July 29, 2003 [6 U.S.C. 482 note]; and

(b) shall cooperate in and facilitate production of reports based on terrorism information with contents and formats that permit dissemination that maximizes the utility of the information in protecting the territory, people, and interests of the United States.

SEC. 3. *Preparing Terrorism Information for Maximum Distribution.* To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the common standards for the sharing of terrorism information established pursuant to section 3 of Executive Order 13356 of August 27, 2004 [formerly set out above], shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 4. *Requirements for Collection of Terrorism Information Inside the United States.* To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the recommendations regarding the establishment of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information collected within the United States made pursuant to section 4 of Executive Order 13356 [formerly set out above] shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 5. *Establishment and Functions of Information Sharing Council.* (a) Consistent with section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004, there is hereby established an Information Sharing Council (Council), chaired by the Program Manager to whom section 1016 of such Act refers, and composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget; the Director of the Federal Bureau of Investigation; the Director of the National Counterterrorism Center; and such other heads of departments or agencies as the Director of National Intelligence may designate.

(b) The mission of the Council is to (i) provide advice and information concerning the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in section 1 of this order; and (ii) perform the duties set forth in section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004.

(c) To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the plan for establishment of a proposed interoperable terrorism information sharing environment reported under section 5(c) of Executive Order 13356 [formerly set out above] shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 6. *Definitions.* As used in this order:

(a) the term “agency” has the meaning set forth for the term “executive agency” in section 105 of title 5, United States Code, together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office; and

(b) the term “terrorism information” has the meaning set forth for such term in section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 7. *General Provisions.* (a) This order:

(i) shall be implemented in a manner consistent with applicable law, including Federal law protecting the information privacy and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the authority of the principal officers of agencies as heads of their respective agencies, including under section 199 of the Revised Statutes (22 U.S.C. 2651), section

201 of the Department of Energy Organization Act (42 U.S.C. 7131), section 103 of the National Security Act of 1947 (50 U.S.C. 403-3) [now 50 U.S.C. 3025], section 102(a) of the Homeland Security Act of 2002 (6 U.S.C. 112(a)), and sections 301 of title 5, 113(b) and 162(b) of title 10, 1501 of title 15, 503 of title 28, and 301(b) of title 31, United States Code;

(iii) shall be implemented consistent with the Presidential Memorandum of June 2, 2005, on “Strengthening Information Sharing, Access, and Integration—Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment;” [not set out in the Code]

(iv) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(v) shall be implemented in a manner consistent with section 102A of the National Security Act of 1947 [50 U.S.C. 3024].

(b) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

SEC. 8. *Amendments and Revocation.* (a) [Amended Ex. Ord. No. 13311, set out as a note under section 482 of this title.]

(b) Executive Order 13356 of August 27, 2004 [formerly set out above], is hereby revoked.

GEORGE W. BUSH.

#### ASSIGNMENT OF CERTAIN FUNCTIONS UNDER THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

Memorandum of President of the United States, Nov. 14, 2006, 71 F.R. 67029, provided:

Memorandum for the Director of National Intelligence

By the authority vested in me as President by the Constitution and laws of the United States, including section 301 of title 3, United States Code, the reporting function of the President under section 1016(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3638) is hereby assigned to the Director of National Intelligence (Director).

The Director shall perform such function in a manner consistent with the President’s constitutional authority to withhold information the disclosure of which could impair foreign relations, national security, the deliberative processes of the Executive, or the performance of the Executive’s constitutional duties.

Any reference in this memorandum to the provision of any Act shall be deemed to include references to any hereafter-enacted provision of law that is the same or substantially the same as such provision.

You are authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

Memorandum of President of the United States, Apr. 10, 2007, 72 F.R. 18561, provided:

Memorandum for the Director of National Intelligence

By the authority vested in me as President by the Constitution and laws of the United States of America, including section 301 of title 3, United States Code, the functions of the President under section 1016(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) (the “Act”) are hereby assigned to the Director of National Intelligence (Director).

The Director shall perform such functions in a manner consistent with direction and guidance issued by the President, including (1) the Memorandum for the Heads of Executive Departments and Agencies of June 2, 2005, entitled “Strengthening Information Sharing,

Access, and Integration—Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment,” and (2) the Memorandum for the Heads of Executive Departments and Agencies of December 16, 2005, entitled “Guidelines and Requirements in Support of the Information Sharing Environment,” provided that the Director shall ensure that the official within the Office of the Director of National Intelligence previously designated as the program manager responsible for information sharing across the Federal Government pursuant to the Act shall be the assistant to the Director in carrying out the functions delegated by this memorandum.

You are authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

[Pub. L. 116-92, div. E, title LXIV, §6402(a), Dec. 20, 2019, 133 Stat. 2196, amended subsec. (b) of this section by substituting “Director of National Intelligence” for “President”, thereby making the assignment of functions in the memorandum above moot.]

Memorandum of President of the United States, Sept. 8, 2007, 72 F.R. 52279, provided:

Memorandum for the Secretary of State[,] the Secretary of Defense[,] the Attorney General[,] the Secretary of Energy[,] the Secretary of Homeland Security[, and] the Director of National Intelligence

By the authority vested in me as President by the Constitution and laws of the United States, including section 301 of title 3, United States Code, the reporting functions of the President under subsections (h) and (j) of section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) (IRTPA), are hereby assigned to the Director of National Intelligence (Director). The Director shall consult the Secretaries of State, Defense, Energy, Homeland Security, and the Attorney General in performing such functions.

Heads of departments and agencies shall, to the extent permitted by law, furnish to the Director information that the Director requests to perform such functions, in the format and on the schedule specified by the Director.

The Director shall perform such functions in a manner consistent with the President’s constitutional authority to withhold information the disclosure of which could impair foreign relations, national security, the deliberative processes of the Executive, and the performance of the Executive’s constitutional duties.

Any reference in this memorandum to the provision of IRTPA shall be deemed to include references to any hereafter-enacted provision of law that is the same or substantially the same as such provision.

The Director is authorized and directed to publish this memorandum in the Federal Register.

GEORGE W. BUSH.

#### § 486. Limitation of liability

A person who has completed a security awareness training course approved by or operated under a cooperative agreement with the Department of Homeland Security using funds made available in fiscal year 2006 and thereafter or in any prior appropriations Acts, who is enrolled in a program recognized or acknowledged by an Information Sharing and Analysis Center, and who reports a situation, activity or incident pursuant to that program to an appropriate authority, shall not be liable for damages in any action brought in a Federal or State court which result from any act or omission unless such person is guilty of gross negligence or willful misconduct. (Pub. L. 109-90, title V, §541, Oct. 18, 2005, 119 Stat. 2089.)

#### Editorial Notes

##### CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2006, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

#### PART J—SECURE HANDLING OF AMMONIUM NITRATE

#### § 488. Definitions

In this part:

##### (1) Ammonium nitrate

The term “ammonium nitrate” means—

(A) solid ammonium nitrate that is chiefly the ammonium salt of nitric acid and contains not less than 33 percent nitrogen by weight; and

(B) any mixture containing a percentage of ammonium nitrate that is equal to or greater than the percentage determined by the Secretary under section 488a(b) of this title.

##### (2) Ammonium nitrate facility

The term “ammonium nitrate facility” means any entity that produces, sells or otherwise transfers ownership of, or provides application services for ammonium nitrate.

##### (3) Ammonium nitrate purchaser

The term “ammonium nitrate purchaser” means any person who purchases ammonium nitrate from an ammonium nitrate facility.

(Pub. L. 107-296, title VIII, §899A, as added Pub. L. 110-161, div. E, title V, §563(a), Dec. 26, 2007, 121 Stat. 2083.)

#### § 488a. Regulation of the sale and transfer of ammonium nitrate

##### (a) In general

The Secretary shall regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility in accordance with this part to prevent the misappropriation or use of ammonium nitrate in an act of terrorism. Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.

##### (b) Ammonium nitrate mixtures

Not later than 90 days after December 26, 2007, the Secretary, in consultation with the heads of appropriate Federal departments and agencies (including the Secretary of Agriculture), shall, after notice and an opportunity for comment, establish a threshold percentage for ammonium nitrate in a substance.

##### (c) Registration of owners of ammonium nitrate facilities

###### (1) Registration

The Secretary shall establish a process by which any person that—

(A) owns an ammonium nitrate facility is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this part.

###### (2) Registration information

Any person applying to register under paragraph (1) shall submit to the Secretary—