

case of a request for disclosure only if, upon the notification of each foreign government and international organization concerned in accordance with the regulations prescribed under subsection (g)(2), any such government or organization requests in writing that the information not be disclosed for an additional period stated in the request of that government or organization. After the national security official concerned considers the request of the foreign government or international organization, the official shall designate a later date as the date after which the information is not to be withheld under this section. The later date may be extended in accordance with a later request of any such foreign government or international organization under this paragraph.

(e) INFORMATION PROTECTED UNDER OTHER AUTHORITY.—This section does not apply to information or matters that are specifically required in the interest of national defense or foreign policy to be protected against unauthorized disclosure under criteria established by an Executive order and are classified, properly, at the confidential, secret, or top secret level pursuant to such Executive order.

(f) DISCLOSURES NOT AFFECTED.—Nothing in this section shall be construed to authorize any official to withhold, or to authorize the withholding of, information from the following:

(1) Congress.

(2) The Comptroller General, unless the information relates to activities that the President designates as foreign intelligence or counterintelligence activities.

(g) REGULATIONS.—(1) The national security officials referred to in subsection (h)(1) shall each prescribe regulations to carry out this section. The regulations shall include criteria for making the determinations required under subsection (b). The regulations may provide for controls on access to and use of, and special markings and specific safeguards for, a category or categories of information subject to this section.

(2) The regulations shall include procedures for notifying and consulting with each foreign government or international organization concerned about requests for disclosure of information to which this section applies.

(h) DEFINITIONS.—In this section:

(1) The term “national security official concerned” means the following:

(A) The Secretary of Defense, with respect to information of concern to the Department of Defense, as determined by the Secretary.

(B) The Secretary of Homeland Security, with respect to information of concern to the Coast Guard, as determined by the Secretary, but only while the Coast Guard is not operating as a service in the Navy.

(C) The Secretary of Energy, with respect to information concerning the national security programs of the Department of Energy, as determined by the Secretary.

(2) The term “agency” has the meaning given that term in section 552(f) of title 5.

(3) The term “international organization” means the following:

(A) A public international organization designated pursuant to section 1 of the

International Organizations Immunities Act (59 Stat. 669; 22 U.S.C. 288) as being entitled to enjoy the privileges, exemptions, and immunities provided in such Act.

(B) A public international organization created pursuant to a treaty or other international agreement as an instrument through or by which two or more foreign governments engage in some aspect of their conduct of international affairs.

(C) An official mission, except a United States mission, to a public international organization referred to in subparagraph (A) or (B).

(Added Pub. L. 106-398, §1 [[div. A], title X, §1073(a)], Oct. 30, 2000, 114 Stat. 1654, 1654A-277; amended Pub. L. 107-107, div. A, title X, §1048(a)(3), (c)(1), Dec. 28, 2001, 115 Stat. 1222, 1226; Pub. L. 107-296, title XVII, §1704(b)(1), Nov. 25, 2002, 116 Stat. 2314.)

#### REFERENCES IN TEXT

The International Organizations Immunities Act, referred to in subsec. (h)(3)(A), is title I of act Dec. 29, 1945, ch. 652, 59 Stat. 669, as amended, which is classified principally to subchapter XVIII (§288 et seq.) of chapter 7 of Title 22, Foreign Relations and Intercourse. For complete classification of this Act to the Code, see Short Title note set out under section 288 of Title 22 and Tables.

#### AMENDMENTS

2002—Subsec. (h)(1)(B). Pub. L. 107-296 substituted “of Homeland Security” for “of Transportation”.

2001—Subsec. (b)(3)(C). Pub. L. 107-107, §1048(a)(3), substituted “subsection (g)” for “subsection (f)”.

Subsec. (d)(1). Pub. L. 107-107, §1048(c)(1), substituted “October 30, 2000,” for “the date of the enactment of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001”.

#### EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective on the date of transfer of the Coast Guard to the Department of Homeland Security, see section 1704(g) of Pub. L. 107-296, set out as a note under section 101 of this title.

#### § 130d. Treatment under Freedom of Information Act of certain confidential information shared with State and local personnel

Confidential business information and other sensitive but unclassified homeland security information in the possession of the Department of Defense that is shared, pursuant to section 892 of the Homeland Security Act of 2002 (6 U.S.C. 482), with State and local personnel (as defined in such section) shall not be subject to disclosure under section 552 of title 5 by virtue of the sharing of such information with such personnel.

(Added Pub. L. 109-364, div. A, title XIV, §1405(a), Oct. 17, 2006, 120 Stat. 2436.)

#### § 130e. Treatment under Freedom of Information Act of certain critical infrastructure security information

(a) EXEMPTION.—The Secretary of Defense may exempt Department of Defense critical infrastructure security information from disclosure pursuant to section 552(b)(3) of title 5, upon a written determination that—

(1) the information is Department of Defense critical infrastructure security information; and

(2) the public interest consideration in the disclosure of such information does not outweigh preventing the disclosure of such information.

(b) DESIGNATION OF DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE SECURITY INFORMATION.—In addition to any other authority or requirement regarding protection from dissemination of information, the Secretary may designate information as being Department of Defense critical infrastructure security information, including during the course of creating such information, to ensure that such information is not disseminated without authorization. Information so designated is subject to the determination process under subsection (a) to determine whether to exempt such information from disclosure described in such subsection.

(c) INFORMATION PROVIDED TO STATE AND LOCAL GOVERNMENTS.—(1) Department of Defense critical infrastructure security information covered by a written determination under subsection (a) or designated under subsection (b) that is provided to a State or local government shall remain under the control of the Department of Defense.

(2)(A) A State or local law authorizing or requiring a State or local government to disclose Department of Defense critical infrastructure security information that is covered by a written determination under subsection (a) shall not apply to such information.

(B) If a person requests pursuant to a State or local law that a State or local government disclose information that is designated as Department of Defense critical infrastructure security information under subsection (b), the State or local government shall provide the Secretary an opportunity to carry out the determination process under subsection (a) to determine whether to exempt such information from disclosure pursuant to subparagraph (A).

(d) DELEGATION.—The Secretary of Defense may delegate the authority to make a determination under subsection (a) to the Director of Administration and Management.

(e) TRANSPARENCY.—Each determination of the Secretary, or the Secretary's designee, under subsection (a) shall be made in writing and accompanied by a statement of the basis for the determination. All such determinations and statements of basis shall be available to the public, upon request, through the Office of the Director of Administration and Management.

(f) DEFINITION.—In this section, the term “Department of Defense critical infrastructure security information” means sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and han-

dling), and other site-specific information on or relating to installation security.

(Added Pub. L. 112-81, div. A, title X, §1091(a), Dec. 31, 2011, 125 Stat. 1604; amended Pub. L. 114-92, div. A, title X, §1081(a)(2), Nov. 25, 2015, 129 Stat. 1000; Pub. L. 114-328, div. A, title XVI, §1662(b), Dec. 23, 2016, 130 Stat. 2614.)

#### AMENDMENTS

2016—Subsecs. (b), (c), (f). Pub. L. 114-328 added subsecs. (b) and (c), redesignated former subsec. (c) as (f), and struck out former subsec. (b). Prior to amendment, text of subsec. (b) read as follows: “Department of Defense critical infrastructure security information covered by a written determination under subsection (a) that is provided to a State or local government shall remain under the control of the Department of Defense.”

2015—Pub. L. 114-92 substituted “Treatment under Freedom of Information Act of certain critical infrastructure security information” for “Treatment under Freedom of Information Act of critical infrastructure security information” in section catchline.

#### § 130f. Notification requirements for sensitive military operations

(a) IN GENERAL.—The Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military operation conducted under this title no later than 48 hours following such operation.

(b) PROCEDURES.—(1) The Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirements of subsection (a) consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify the congressional defense committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) In the event of an unauthorized disclosure of a sensitive military operation covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the sensitive military operation concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification shall be provided by not later than 48 hours after the provision of the verbal notification.

(c) BRIEFING REQUIREMENT.—The Secretary of Defense shall periodically brief the congressional defense committees on Department of Defense personnel and equipment assigned to sensitive military operations, including Department of Defense support to such operations conducted under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

(d) SENSITIVE MILITARY OPERATION DEFINED.—(1) Except as provided in paragraph (2), in this section, the term “sensitive military operation” means—