§ 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 handling), 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