General may delegate that authority only to the Associate Attorney General or an Assistant Attorney General and only if the Associate Attorney General or Assistant Attorney General to whom delegated has been designated by the Attorney General to act for, and to exercise the general powers of, the Attorney General.

(g) RELATIONSHIP TO OTHER AUTHORITY.—Nothing in this section shall be construed to restrict any executive branch authority regarding use of members of the armed forces or equipment of the Department of Defense that was in effect before September 23, 1996.

(Added Pub. L. 104–201, div. A, title XIV, § 1416(a)(1), Sept. 23, 1996, 110 Stat. 2721; amended Pub. L. 105–85, div. A, title X, § 1073(a)(6), Nov. 18, 1997, 111 Stat. 1900; Pub. L. 111–383, div. A, title X, § 1075(b)(10)(A), (B), Jan. 7, 2011, 124 Stat. 4369; Pub. L. 112–81, div. A, title X, § 1089, Dec. 31, 2011, 125 Stat. 1603.)

AMENDMENTS

2011—Pub. L. 111–383, § 1075(b)(10)(B), struck out ''chemical or biological'' before ''weapons'' in section catchline.

Subsec. (a). Pub. L. 112–81 struck out ''biological or chemical'' before ''weapon of mass destruction'' in introductory provisions.

Pub. L. 111–383, § 1075(b)(10)(A), substituted ''section 175, 229, or 2332a'' for ''section 175 or 2332c''.

Subsec. (b). Pub. L. 112–81 struck out ''biological or chemical'' before ''weapon of mass destruction'' in two places in introductory provisions.

Subsecs. (b)(2)(C), (d)(2)(A)(ii). Pub. L. 111–383, § 1075(b)(10)(A), substituted ''section 175, 229, or 2332a'' for ''section 175 or 2332c''.

1997—Subsec. (g). Pub. L. 105–85 substituted ''September 23, 1996'' for ''the date of the enactment of the National Defense Authorization Act for Fiscal Year 1997''.

MILITARY ASSISTANCE TO CIVIL AUTHORITIES TO RESPOND TO ACT OR THREAT OF TERRORISM

Pub. L. 106–65, div. A, title X, § 1023, Oct. 5, 1999, 113 Stat. 747, authorized the Secretary of Defense, upon the request of the Attorney General, to provide assistance to civil authorities in responding to an act of terrorism or threat of an act of terrorism within the United States, if the Secretary determined that certain conditions were met, subject to reimbursement and limitations on funding and personnel, and provided that this authority applied between Oct. 1, 1999, and Sept. 30, 2004.

§ 383. Situations involving bombings of places of public use, Government facilities, public transportation systems, and infrastructure facilities

(a) IN GENERAL.—Upon the request of the Attorney General, the Secretary of Defense may provide assistance in support of Department of Justice activities related to the enforcement of section 2332f of title 18 during situations involving bombings of places of public use, Government facilities, public transportation systems, and infrastructure facilities.

(b) RENDERING-SAFE SUPPORT.—Military explosive ordnance disposal units providing rendering-safe support to Department of Justice activities relating to the enforcement of section 175, 229, or 2332a of title 18 in emergency situations involving weapons of mass destruction shall provide such support in a manner consistent with the provisions of section 382 of this title.

(c) REGULATIONS.—(1) The Secretary of Defense and the Attorney General shall jointly prescribe regulations concerning the types of assistance that may be provided under this section. Such regulations shall also describe the actions that Department of Defense personnel may take in circumstances incident to the provision of assistance under this section.

(2)(A) Except as provided in subparagraph (B), the regulations prescribed under paragraph (1) may not authorize any of the following actions:

(i) Arrest.

(ii) Any direct participation in conducting a search for or seizure of evidence related to a violation of section 175, 229, or 2332a of title 18.

(iii) Any direct participation in the collection of intelligence for law enforcement purposes.

(B) Such regulations may authorize an action described in subparagraph (A) to be taken under the following conditions:

(i) The action is considered necessary for the immediate protection of human life, and civilian law enforcement officials are not capable of taking the action.

(ii) The action is otherwise authorized under subsection (a) or under otherwise applicable law.

(d) EXPLOSIVE ORDNANCE DEFINED.—The term ''explosive ordnance''—

(1) means—

(A) bombs and warheads;

(B) guided and ballistic missiles;

(C) artillery, mortar, rocket, and small arms ammunition;

(D) all mines, torpedoes, and depth charges;

(E) grenades demolition charges;

(F) pyrotechnics;

(G) clusters and dispensers;

(H) cartridge- and propellant- actuated devices;

(I) electroexplosives devices;

(J) clandestine and improvised explosive devices; and

(K) all similar or related items or components explosive in nature; and

(2) includes all munitions containing explosives, propellants, nuclear fission or fusion materials, and biological and chemical agents.

(Added Pub. L. 114–92, div. A, title X, § 1082(a), Nov. 25, 2015, 129 Stat. 1002.)

CHAPTER 19—CYBER MATTERS

AMENDMENTS

2015—Pub. L. 114–92, div. A, title X, § 1081(a)(4), title XVI, § 1641(c)(2), Nov. 25, 2015, 129 Stat. 1001, 1116, substituted ''Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors'' for

''Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors'' in item 391 and added item 393.

2014—Pub. L. 113–291, div. A, title XVI, §1633(d), Dec. 19, 2014, 128 Stat. 3643, added item 392.

§ 391. Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors

(a) DESIGNATION OF DEPARTMENT COMPONENT TO RECEIVE REPORTS.—The Secretary of Defense shall designate a component of the Department of Defense to receive reports of cyber incidents from contractors in accordance with this section and section 393 of this title or from other governmental entities.

(b) PROCEDURES FOR REPORTING CYBER INCIDENTS.—The Secretary of Defense shall establish procedures that require an operationally critical contractor to report in a timely manner to component designated under subsection (a) each time a cyber incident occurs with respect to a network or information system of such operationally critical contractor.

(c) PROCEDURE REQUIREMENTS.—

(1) DESIGNATION AND NOTIFICATION.—The procedures established pursuant to subsection (a) shall include a process for—

(A) designating operationally critical contractors; and

(B) notifying a contractor that it has been designated as an operationally critical contractor.

(2) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each operationally critical contractor to rapidly report to the component of the Department designated pursuant to subsection (d)(2)(A) on each cyber incident with respect to any network or information systems of such contractor. Each such report shall include the following:

(A) An assessment by the contractor of the effect of the cyber incident on the ability of the contractor to meet the contractual requirements of the Department.

(B) The technique or method used in such cyber incident.

(C) A sample of any malicious software, if discovered and isolated by the contractor, involved in such cyber incident.

(D) A summary of information compromised by such cyber incident.

(3) DEPARTMENT ASSISTANCE AND ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT PERSONNEL.—The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for Department personnel to, if requested, assist operationally critical contractors in detecting and mitigating penetrations; and

(B) provide that an operationally critical contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated.

(4) PROTECTION OF TRADE SECRETS AND OTHER INFORMATION.—The procedures established pursuant to subsection (a) shall provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

(5) DISSEMINATION OF INFORMATION.—The procedures established pursuant to subsection (a) shall limit the dissemination of information obtained or derived through the procedures to entities—

(A) with missions that may be affected by such information;

(B) that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(C) that conduct counterintelligence or law enforcement investigations; or

(D) for national security purposes, including cyber situational awareness and defense purposes.

(d) PROTECTION FROM LIABILITY OF OPERATIONALLY CRITICAL CONTRACTORS.—(1) No cause of action shall lie or be maintained in any court against any operationally critical contractor, and such action shall be promptly dismissed, for compliance with this section that is conducted in accordance with procedures established pursuant to subsection (b).

(2)(A) Nothing in this section shall be construed—

(i) to require dismissal of a cause of action against an operationally critical contractor that has engaged in willful misconduct in the course of complying with the procedures established pursuant to subsection (b); or

(ii) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(B) In any action claiming that paragraph (1) does not apply due to willful misconduct described in subparagraph (A), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each operationally critical contractor subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(C) In this subsection, the term ''willful misconduct'' means an act or omission that is taken—

(i) intentionally to achieve a wrongful purpose;

(ii) knowingly without legal or factual justification; and

(iii) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

(e) DEFINITIONS.—In this section:

(1) CYBER INCIDENT.—The term ''cyber incident'' means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

(2) OPERATIONALLY CRITICAL CONTRACTOR.—The term ''operationally critical contractor'' means a contractor designated by the Secretary for purposes of this section as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support