stituted ''Except as provided in paragraph (2), if any information'' for ''If any information'', and added par. (2).

Subsec. (e). Pub. L. 114–328, §1251(f), inserted ''that may also include other sensitive information'' after ''annex''.

EFFECTIVE DATE OF 2016 AMENDMENT

Pub. L. 114–328, div. A, title XII, §1246(d)(2), Dec. 23, 2016, 130 Stat. 2521, provided that the amendment made by section 1246(d)(2)(A) is effective as of January 1, 2020.

CHAPTER 19—CYBER MATTERS

AMENDMENTS

2018—Pub. L. 115–232, div. A, title XVI, §1631(c)(2), Aug. 13, 2018, 132 Stat. 2123, added items 394 to 396.

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