

ment the requirements of Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity), including changes to the Federal Acquisition Regulations and remedies to include suspension and debarment.

(h) Savings provision

Nothing in this section shall be construed to supersede or to abrogate, modify, or otherwise limit the authority that is vested in any officer or any agency of the United States Government to regulate or take action with respect to the cybersecurity of an entity.

(Pub. L. 107–296, title XXII, § 2242, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1042.)

Editorial Notes

REFERENCES IN TEXT

Section 681(14)(A) of this title, referred to in subsec. (c)(2)(C)(ii), was repealed by section 7143(b)(2)(N)(v) of Pub. L. 117–263. See section 650(22)(A) of this title. References to terms defined in this chapter deemed to be references to those terms as defined in section 650 of this title, see section 7143(f)(2) of Pub. L. 117–263, set out as a Rule of Construction note under section 650 of this title.

Executive Order 14028, referred to in subsec. (g), is Ex. Ord. No. 14028, May 12, 2021, 86 F.R. 26633, which is set out as a note under section 3551 of Title 44, Public Printing and Documents.

§ 681c. Voluntary reporting of other cyber incidents

(a) In general

Entities may voluntarily report cyber incidents or ransom payments to the Agency that are not required under paragraph (1), (2), or (3) of section 681b(a) of this title, but may enhance the situational awareness of cyber threats.

(b) Voluntary provision of additional information in required reports

Covered entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 681b(a) of this title information that is not required to be included, but may enhance the situational awareness of cyber threats.

(c) Application of section 681e of this title

Section 681e of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b) as it applies to reports and information submitted under section 681b of this title.

(Pub. L. 107–296, title XXII, § 2243, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1049; amended Pub. L. 117–263, div. G, title LXXI, § 7143(e)(1), Dec. 23, 2022, 136 Stat. 3664.)

Editorial Notes

AMENDMENTS

2022—Subsec. (c). Pub. L. 117–263 added subsec. (c) and struck out former subsec. (c). Prior to amendment, text read as follows: “The protections under section 681e of this title applicable to reports made under section 681b of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).”

§ 681d. Noncompliance with required reporting

(a) Purpose

In the event that a covered entity that is required to submit a report under section 681b(a) of this title fails to comply with the requirement to report, the Director may obtain information about the cyber incident or ransom payment by engaging the covered entity directly to request information about the cyber incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the covered entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred.

(b) Initial request for information

(1) In general

If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 681a(a) of this title, that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such cyber incident or payment to the Agency in accordance with section 681b(a) of this title, the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

(2) Treatment

Information provided to the Agency in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 681b of this title¹ including that section 681e of this title shall apply to such information in the same manner and to the same extent to information submitted in response to requests under paragraph (1) as it applies to information submitted under section 681b of this title.

(c) Enforcement

(1) In general

If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the covered entity from which such information was requested, or received an inadequate response, the Director may issue to such covered entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 681b of this title and any implementing regulations, and assess potential impacts to national security, economic security, or public health and safety.

(2) Civil action

(A) In general

If a covered entity fails to comply with a subpoena, the Director may refer the matter

¹ So in original. Probably should be followed by a comma.