service to customers to make or facilitate ransom payments on behalf of covered entities impacted by ransomware attacks and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

(2) Elements

The outreach and education campaign under paragraph (1) shall include the following:

(A) An overview of the final rule issued pursuant to subsection (b).

(B) An overview of mechanisms to submit to the Agency covered cyber incident reports, ransom payment reports, and information relating to the disclosure, retention, and use of covered cyber incident reports and ransom payment reports under this section.

(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

(D) An overview of the steps taken under section 681d of this title when a covered entity is not in compliance with the reporting requirements under subsection (a).

(E) Specific outreach to cybersecurity vendors, cyber incident response providers, cybersecurity insurance entities, and other entities that may support covered entities.

(F) An overview of the privacy and civil liberties requirements in this part.

(3) Coordination

In conducting the outreach and education campaign required under paragraph (1), the Agency may coordinate with—

(A) the Critical Infrastructure Partnership Advisory Council established under section 451 of this title;

(B) Information Sharing and Analysis Organizations;

(C) trade associations;

(D) information sharing and analysis centers;

(E) sector coordinating councils; and

(F) any other entity as determined appropriate by the Director.

(f) Exemption

Sections 3506(c), 3507, 3508, and 3509 of title 44 shall not apply to any action to carry out this section.

(g) Rule of construction

Nothing in this section shall affect the authorities of the Federal Government to implement 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 title[1] 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 to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

(B) Venue

An action under this paragraph may be brought in the judicial district in which the covered entity against which the action is brought resides, is found, or does business.

(C) Contempt of court

A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

(3) Non-delegation

The authority of the Director to issue a subpoena under this subsection may not be delegated.

(4) Authentication

(A) In general

Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

(B) Invalid if not authenticated

Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

(d) Provision of certain information to Attorney General

(1) In general

Notwithstanding section 681e(a)(5) of this title and paragraph (b)(2) of this section, if the Director determines, based on the information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide such information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use such information for a regulatory enforcement action or criminal prosecution.

(2) Consultation

The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making the determination under paragraph (1).

(e) Considerations

When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

(1) the complexity in determining if a covered cyber incident has occurred; and

(2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

(f) Exclusions

This section shall not apply to a State, local, Tribal, or territorial government entity.

(g) Report to Congress

The Director shall submit to Congress an annual report on the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b);

(2) issued a subpoena pursuant to subsection (c); or

(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

(h) Publication of the annual report

The Director shall publish a version of the annual report required under subsection (g) on the

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

website of the Agency, which shall include, at a minimum, the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b); or

(2) issued a subpoena pursuant to subsection (c).

(i) Anonymization of reports

The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

(Pub. L. 107–296, title XXII, § 2244, 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)(2), Dec. 23, 2022, 136 Stat. 3664.)

Editorial Notes

AMENDMENTS

2022—Subsec. (b)(2). Pub. L. 117–263 inserted ''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'' after ''section 681b of this title''.

§ 681e. Information shared with or provided to the Federal Government

(a) Disclosure, retention, and use

(1) Authorized activities

Information provided to the Agency pursuant to section 681b or 681c of this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(A) a cybersecurity purpose;

(B) the purpose of identifying—

(i) a cyber threat, including the source of the cyber threat; or

(ii) a security vulnerability;

(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 681b or 681c of this title or any of the offenses listed in section 1504(d)(5)(A)(v) of this title.

(2) Agency actions after receipt

(A) Rapid, confidential sharing of cyber threat indicators

Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Agency shall immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

(B) Principles for sharing security vulnerabilities

With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

(3) Privacy and civil liberties

Information contained in covered cyber incident and ransom payment reports submitted to the Agency pursuant to section 681b of this title shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 1504 of this title and in a manner that protects personal information from unauthorized use or unauthorized disclosure.

(4) Digital security

The Agency shall ensure that reports submitted to the Agency pursuant to section 681b of this title, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

(5) Prohibition on use of information in regulatory actions

(A) In general

A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency in accordance with this part to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity.

(B) Clarification

A report submitted to the Agency pursuant to section 681b or 681c of this title may, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems.