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.

(b) Protections for reporting entities and information

Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 681b of this title, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant to section 681c of this title, shall—

(1) be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;

(2) be exempt from disclosure under section 552(b)(3) of title 5 (commonly known as the ''Freedom of Information Act''), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

(3) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and

(4) not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(c) Liability protections

(1) In general

No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 681b(a) of this title that is submitted in conformance with this part and the rule promulgated under section 681b(b) of this title, except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 681d(c)(2) of this title.

(2) Scope

The liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency.

(3) Restrictions

Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this part or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this part shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

(d) Sharing with non-Federal entities

The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 681b of this title available to critical infrastructure owners and operators and the general public.

(e) Stored Communications Act

Nothing in this part shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18 (commonly known as the ''Stored Communications Act'').

(Pub. L. 107–296, title XXII, § 2245, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1051.)

§ 681f. Cyber Incident Reporting Council

(a) Responsibility of the Secretary

The Secretary shall lead an intergovernmental Cyber Incident Reporting Council, in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations.

(b) Rule of construction

Nothing in subsection (a) shall be construed to provide any additional regulatory authority to any Federal entity.

(Pub. L. 107–296, title XXII, § 2246, as added Pub. L. 117–103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1054.)

§ 681g. Federal sharing of incident reports

(a) Cyber incident reporting sharing

(1) In general

Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Agency as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Department of Homeland Security (including the Cybersecurity and Infrastructure Security Agency) and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 681a(b) of this title, as added by section 103 of this division.

(2) Rule of construction

The requirements described in paragraph (1) and section 681e(d) of this title, as added by section 103 of this division, may not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure or provision of information within the executive branch.

(3) Protection of information

The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection re-