

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 requirements than this division or the amendments made by this division.

(4) Effective date

This subsection shall take effect on the effective date of the final rule issued pursuant to section 681b(b) of this title, as added by section 103 of this division.

(5) Agency agreements

(A) In general

The Agency and any Federal agency, including any independent establishment (as defined in section 104 of title 5), that receives incident reports from entities, including due to ransomware attacks, shall, as appropriate, enter into a documented agreement to establish policies, processes, procedures, and mechanisms to ensure reports are shared with the Agency pursuant to paragraph (1).

(B) Availability

To the maximum extent practicable, each documented agreement required under subparagraph (A) shall be made publicly available.

(C) Requirement

The documented agreements required by subparagraph (A) shall require reports be shared from Federal agencies with the Agency in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments established in section 681b of this title, as added by section 103 of this division.

(b) Harmonizing reporting requirements

The Secretary of Homeland Security, acting through the Director, shall, in consultation with the Cyber Incident Reporting Council described in section 681f of this title, as added by section 103 of this division, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with appropriate Federal partners and regulatory authorities that receive reports relating to incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agree-

ments between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of the Agency to gain timely situational awareness of a covered cyber incident or ransom payment.

(Pub. L. 117–103, div. Y, §104, Mar. 15, 2022, 136 Stat. 1054.)

Editorial Notes

REFERENCES IN TEXT

Section 103 of this division, referred to in text, is section 103 of div. Y of Pub. L. 117–103, which enacted this part and amended section 659 of this title.

CODIFICATION

Section was enacted as part of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, and also as part of the Consolidated Appropriations Act, 2022, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of terms used in this section, see section 102 of div. Y of Pub. L. 117–103, which is set out as a note under section 665j of this title.

CHAPTER 2—NATIONAL EMERGENCY MANAGEMENT

Sec.

701. Definitions.

SUBCHAPTER I—PERSONNEL PROVISIONS

PART A—FEDERAL EMERGENCY MANAGEMENT AGENCY PERSONNEL

711. Surge Capacity Force.

PART B—EMERGENCY MANAGEMENT CAPABILITIES

- 721. Evacuation preparedness technical assistance.
- 722. Urban Search and Rescue Response System.
- 723. Metropolitan Medical Response Grant Program.
- 724. Logistics.
- 725. Prepositioned equipment program.
- 726. Basic life supporting first aid and education.
- 727. Improvements to information technology systems.
- 728. Disclosure of certain information to law enforcement agencies.

SUBCHAPTER II—COMPREHENSIVE PREPAREDNESS SYSTEM

PART A—NATIONAL PREPAREDNESS SYSTEM

- 741. Definitions.
- 742. National preparedness.
- 743. National preparedness goal.
- 744. Establishment of national preparedness system.
- 745. National planning scenarios.
- 746. Target capabilities and preparedness priorities.
- 747. Equipment and training standards.
- 748. Training and exercises.
- 748a. Prioritization of facilities.
- 749. Comprehensive assessment system.
- 750. Remedial action management program.
- 751. Federal response capability inventory.
- 752. Reporting requirements.
- 753. Federal preparedness.
- 754. Use of existing resources.

Sec.

PART B—ADDITIONAL PREPAREDNESS

- 761. Emergency Management Assistance Compact grants.
- 762. Emergency management performance grants program.
- 763. Transfer of Noble Training Center.
- 763a. Training for Federal Government, foreign governments, or private entities.
- 764. National exercise simulation center.
- 765. Real property transactions.

PART C—MISCELLANEOUS AUTHORITIES

- 771. National Disaster Recovery Strategy.
- 772. National Disaster Housing Strategy.
- 773. Individuals with disabilities guidelines.
- 774. Reunification.
- 775. National Emergency Family Registry and Locator System.
- 776. Individuals and households pilot program.
- 777. Public assistance pilot program.

PART D—PREVENTION OF FRAUD, WASTE, AND ABUSE

- 791. Advance contracting.
- 792. Repealed.
- 793. Oversight and accountability of Federal disaster expenditures.
- 794. Limitation on length of certain noncompetitive contracts.
- 795. Fraud, waste, and abuse controls.
- 796. Registry of disaster response contractors.
- 797. Fraud prevention training program.

PART E—AUTHORIZATION OF APPROPRIATIONS

- 811. Authorization of appropriations.

PART F—GLOBAL CATASTROPHIC RISK MANAGEMENT

- 821. Definitions.
- 822. Assessment of global catastrophic risk.
- 823. Report required.
- 824. Enhanced catastrophic incident annex.
- 825. Rules of construction.

§ 701. Definitions

In this title—¹

(1) the term “Administrator” means the Administrator of the Agency;

(2) the term “Agency” means the Federal Emergency Management Agency;

(3) the term “appropriate committees of Congress” means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) those committees of the House of Representatives that the Speaker of the House of Representatives determines appropriate;

(4) the term “catastrophic incident” means any natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area;

(5) the term “Department” means the Department of Homeland Security;

(6) the terms “emergency” and “major disaster” have the meanings given the terms in section 5122 of title 42;

(7) the term “emergency management” means the governmental function that coordinates and integrates all activities necessary to

¹ See References in Text note below.