6 USCS § 681a

Current through Public Law 118-62, approved May 13, 2024.

United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 1. HOMELAND SECURITY ORGANIZATION (§§ 101 — 681g) > CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (§§ 650 — 681g) > CYBER INCIDENT REPORTING (§§ 681 — 681g)

§ 681a. Cyber incident review

(a) Activities. The Center shall—

(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors;

(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

(3) leverage information gathered about cyber incidents to—

(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2245 [6 USCS § 681e];

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments,

particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(7) with respect to covered cyber incident reports under section 2242(a) and 2243 [6 USCS §§ 681b(a) and 681c] involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

(9) proactively identify opportunities, consistent with the protections in section 2245 [6 USCS § 681e], to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

(10) in accordance with section 2245 [6 USCS § 681e] and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2243 [6 USCS § 681c], or information received pursuant to a request for information or subpoena under section 2244 [6 USCS § 681d], make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

(b) Interagency sharing. The President or a designee of the President—

(1) may establish a specific time requirement for sharing information under subsection (a)(10); and

(2) shall determine the appropriate Federal agencies under subsection (a)(10).

(c) Periodic briefing. Not later than 60 days after the effective date of the final rule required under section 2242(b) [6 USCS § 681b(b)], and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

(1) include the total number of reports submitted under sections 2242 and 2243 [6 USCS §§ 681b and 681c] during the preceding month, including a breakdown of required and voluntary reports;

(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2242 and 2243 [6 USCS §§ 681b and 681c], including—

(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

(3) include a summary of the known uses of the information in reports submitted under sections 2242 and 2243 [6 USCS §§ 681b and 681c]; and

(4) include an unclassified portion, but may include a classified component.

History

Nov. 25, 2002, P.L. 107-296, Title XXII, Subtitle D, § 2241, as added March 15, 2022, P.L. 117-103, Div Y, § 103(a)(2), 136 Stat. 1040.