6 USCS § 660

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) > CYBERSECURITY AND INFRASTRUCTURE SECURITY (§§ 651 — 665n)

§ 660. Cybersecurity plans

(a) Definitions. In this section, the term "agency information system" means an information system used or operated by an agency or by another entity on behalf of an agency.

(b) Intrusion assessment plan.

(1) Requirement. The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) Exception. The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) Cyber incident response plan. The Director of the Cybersecurity and Infrastructure Security Agency shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, update not less often than biennially, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate such stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response.

(d) National Response Framework. The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(e) Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

(1) In general.

(A) Requirement. Not later than one year after the date of the enactment of this subsection [enacted Dec. 27, 2021], the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

(B) Recommendations and requirements. The strategy required under subparagraph (A) shall provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents.

(2) Contents. The strategy required under paragraph (1) shall—

(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

(i) incident exercises, information sharing and incident notification procedures;

(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

(iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40, United States Code;

(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents; and

(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect,

respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

(3) Considerations. In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, shall consider—

(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems owned or operated by State, local, Tribal, and territorial governments; and

(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies.

(4) Exemption. Chapter 35 of title 44, United States Code [44 USCS §§ 3501 et seq.] (commonly known as the "Paperwork Reduction Act"), shall not apply to any action to implement this subsection.

History

HISTORY:

Nov. 25, 2002, P. L. 107-296, Title XXII [II], Subtitle A [C], § 2210 [228], as added and amended Dec. 18, 2015, P. L. 114-113, Div N, Title II, Subtitle A, § 205, Subtitle B, § 223(a)(2), (4)–(6), 129 Stat. 2961, 2963; Nov. 16, 2018, P.L. 115-278, § 2(g)(2)(I), (9)(A)(iv), 132 Stat. 4178, 4181; Dec. 27, 2021, P.L. 117-81, Div A, Title XV, Subtitle C, §§ 1545, 1546, 135 Stat. 2057, 2059; Dec. 23, 2022, P.L. 117-263, Div G, Title LXXI, Subtitle E, § 7143(b)(2)(E), (c)(8), 136 Stat. 3660, 3663.