''(2) the term 'critical infrastructure' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

''(3) the term 'cybersecurity risk' has the meaning given that term in section 226 [2209] of the Homeland Security Act of 2002, as added by section 3;

''(4) the term 'information sharing and analysis organization' has the meaning given that term in section 212(5) [renumbered 2222(5) by section 2(g)(2)(H) of Pub. L. 115–278] of the Homeland Security Act of 2002 ([former] 6 U.S.C. 131(5)) [now 6 U.S.C. 671(5); see 6 U.S.C. 650(13)];

''(5) the term 'information system' has the meaning given that term in section 3502(8) of title 44, United States Code; and

''(6) the term 'Secretary' means the Secretary of Homeland Security.''

§ 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 December 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;

(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and terri-

torial 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 (commonly known as the ''Paperwork Reduction Act'') shall not apply to any action to implement this subsection.

(Pub. L. 107–296, title XXII, § 2210, formerly title II, § 228, as added and amended Pub. L. 114–113, div. N, title II, §§ 205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964; renumbered title XXII, § 2210, and amended Pub. L. 115–278, § 2(g)(2)(I), (9)(A)(iv), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 117–81, div. A, title XV, §§ 1545, 1546, Dec. 27, 2021, 135 Stat. 2057, 2059; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(E), (c)(8), Dec. 23, 2022, 136 Stat. 3660, 3663.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 149 of this title prior to renumbering by Pub. L. 115–278.

Former section 149 of this title, which was transferred and redesignated as subsec. (c) of this section by Pub. L. 114–113, div. N, title II, § 223(a)(2), Dec. 18, 2015, 129 Stat. 2963, was based on Pub. L. 107–296, title II, § 227, as added by Pub. L. 113–282, § 7(a), Dec. 18, 2014, 128 Stat. 3070.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, § 7143(b)(2)(E)(i), substituted ''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.'' for ''section—'' and struck out pars. (1) to (4) which defined agency information system, cybersecurity risk, information system, intelligence community, and national security system.

Subsec. (c). Pub. L. 117–263, § 7143(c)(8), substituted ''Director of the Cybersecurity and Infrastructure Security Agency'' for ''Director of Cybersecurity and Infrastructure Security''.

Pub. L. 117–263, § 7143(b)(2)(E)(ii), substituted ''Information Sharing and Analysis Organizations'' for ''information sharing and analysis organizations (as defined in section 671(5) of this title)'' and struck out ''(as defined in section 659 of this title)'' after ''cybersecurity risks''.

Subsec. (e)(1)(B). Pub. L. 117–263, § 7143(b)(2)(E)(iii)(I), which directed striking out ''(as such term is defined in section 659 of this title)'', was executed by striking out ''(as such term is defined in section 659 of this title)'' after ''cybersecurity risks'' and after ''incidents'', to reflect the probable intent of Congress.

Subsec. (e)(3)(C). Pub. L. 117–263, § 7143(b)(2)(E)(iii)(II), struck out ''(as such term is defined in section 1501 of this title)'' after ''information systems''.

2021—Subsec. (c). Pub. L. 117–81, § 1546, substituted ''update not less often than biennially'' for ''regularly update'' and inserted ''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.'' at end.

Subsec. (e). Pub. L. 117–81, § 1545, added subsec. (e).

2018—Subsec. (a)(2). Pub. L. 115–278, § 2(g)(9)(A)(iv)(I), substituted ''section 659 of this title'' for ''section 148 of this title''.

Subsec. (c). Pub. L. 115–278, § 2(g)(9)(A)(iv), substituted ''Director of Cybersecurity and Infrastructure Security'' for ''Under Secretary appointed under section 113(a)(1)(H) of this title'', ''section 671(5) of this title'' for ''section 131(5) of this title'', and ''section 659 of this title'' for ''section 148 of this title''.

2015—Subsec. (c). Pub. L. 114–113, § 223(a)(5), made technical amendment to reference in original act which appears in text as reference to section 148 of this title.

Pub. L. 114–113, § 223(a)(2), transferred former section 149 of this title to subsec. (c) of this section. See Codification note above.

Subsec. (d). Pub. L. 114–113, § 205, added subsec. (d).

Statutory Notes and Related Subsidiaries

RULES OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, see section 7143(f)(1) of Pub. L. 117–263, set out as a note under section 650 of this title.

Pub. L. 113–282, § 7(c), Dec. 18, 2014, 128 Stat. 3072, provided that: ''Nothing in the amendment made by subsection (a) [enacting subsec. (c) of this section and section 150 of this title] or in subsection (b)(1) [formerly classified as a note under section 3543 of Title 44, Public Printing and Documents, see now section 2(d)(1) of Pub. L. 113–283, set out as a note under section 3553 of Title 44] shall be construed to alter any authority of a Federal agency or department.''

§ 661. Cybersecurity strategy

(a) In general

Not later than 90 days after December 23, 2016, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.