6 USCS § 1533

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

United States Code Service > TITLE 6. DOMESTIC SECURITY (§§ 101 — 1534) > CHAPTER 6. CYBERSECURITY (§§ 1500 — 1534) > OTHER CYBER MATTERS (§§ 1531 — 1534)

§ 1533. Improving cybersecurity in the health care industry

(a) Definitions. In this section:

(1) Appropriate congressional committees. The term "appropriate congressional committees" means—

(A) the Committee on Health, Education, Labor, and Pensions, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) Business associate. The term "business associate" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before the date of the enactment of this Act [enacted Dec. 18, 2015]).

(3) Covered entity. The term "covered entity" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before the date of the enactment of this Act [enacted Dec. 18, 2015]).

(4) Cybersecurity threat; cyber threat indicator; defensive measure; Federal entity; non-Federal entity; private entity. The terms "cybersecurity threat", "cyber threat indicator", "defensive measure", "Federal entity", "non-Federal entity", and "private entity" have the meanings given such terms in section 102 of this division [6 USCS § 1501].

(5) Health care clearinghouse; health care provider; health plan. The terms "health care clearinghouse", "health care provider", and "health plan" have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before the date of the enactment of this Act [enacted Dec. 18, 2015]).

(6) Health care industry stakeholder. The term "health care industry stakeholder" means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) advocate for patients or consumers;

(C) pharmacist;

(D) developer or vendor of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

(7) Secretary. The term "Secretary" means the Secretary of Health and Human Services.

(b) Report.

(1) In general. Not later than 1 year after the date of enactment of this Act [enacted Dec. 18, 2015], the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.

(2) Contents of report. With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report under paragraph (1) shall include—

(A) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(B) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

(c) Health care industry cybersecurity task force.

(1) In general. Not later than 90 days after the date of the enactment of this Act [enacted Dec. 18, 2015], the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing title I of this division [6 USCS §§ 1501 et seq.], so that the Federal Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) Termination. The task force established under this subsection shall terminate on the date that is 1 year after the date on which such task force is established.

(3) Dissemination. Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(d) Aligning health care industry security approaches.

(1) In general. The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that—

(A) serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) are consistent with—

(i) the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));

(ii) the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and

(iii) the provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and

(D) are updated on a regular basis and applicable to a range of health care organizations.

(2) Limitation. Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase, on compliance with this subsection.

(3) No liability for nonparticipation. Nothing in this section shall be construed to subject a health care industry stakeholder to liability for choosing not to engage in the voluntary activities authorized or guidelines developed under this subsection.

(e) Incorporating ongoing activities. In carrying out the activities under this section, the Secretary may incorporate activities that are ongoing as of the day before the date of enactment of this Act [enacted Dec. 18, 2015] and that are consistent with the objectives of this section.

(f) Rule of construction. Nothing in this section shall be construed to limit the antitrust exemption under section 104(e) [6 USCS § 1503(e)] or the protection from liability under section 106 [6 USCS § 1505].

History

HISTORY:

Dec. 18, 2015, P. L. 114-113, Div N, Title IV, § 405, 129 Stat. 2981.