(§§ 231–237) of title II of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2159, which enacted part D (§ 161 et seq.) of subchapter II of chapter 1 of this title and amended sections 3712 and 3722 of Title 42, The Public Health and Welfare. For complete classification of subtitle D to the Code, see Tables.

§ 1525. Termination

(a) In general

The authority provided under section 151 of this title, and the reporting requirements under section 1524(c) of this title shall terminate on the date that is 7 years after December 18, 2015.

(b) Rule of construction

Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 151(d)(2) of this title, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

(Pub. L. 114–113, div. N, title II, § 227, Dec. 18, 2015, 129 Stat. 2971.)

SUBCHAPTER III—OTHER CYBER MATTERS

§ 1531. Apprehension and prosecution of international cyber criminals

(a) International cyber criminal defined

In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) Consultations for noncooperation

The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) Annual report

(1) In general

The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) Form

The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

(3) Appropriate congressional committees

For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(Pub. L. 114–113, div. N, title IV, § 403, Dec. 18, 2015, 129 Stat. 2979.)

§ 1532. Enhancement of emergency services

(a) Collection of data

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, acting through the center established under section 148 of this title, in coordination with appropriate Federal entities and the Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 101 of this title) within the State.

(b) Analysis of data

Not later than 1 year after December 18, 2015, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, and in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations

on security and resilience measures for any information system or network used by State emergency response providers.

(c) Best practices

(1) In general

Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 272(e) of title 15.

(2) Report

The Director of the National Institute of Standards and Technology shall submit to Congress a report on the result of the activities of the Director under paragraph (1), including any methods developed by the Director under such paragraph, and shall make such report publicly available on the website of the National Institute of Standards and Technology.

(d) Rule of construction

Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require a non-Federal entity (as defined in section 1501 of this title) to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the result of the activities carried out under subsection (c), including any methods developed under such subsection.

(Pub. L. 114–113, div. N, title IV, §404, Dec. 18, 2015, 129 Stat. 2980.)

§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 December 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 December 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 1501 of this title.

(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 December 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 December 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.