

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 272(c)(15) of title 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 December 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 1503(e) of this title or the protection from liability under section 1505 of this title.

(Pub. L. 114-113, div. N, title IV, § 405, Dec. 18, 2015, 129 Stat. 2981.)

## **Editorial Notes**

### **REFERENCES IN TEXT**

Section 264(c) of the Health Insurance Portability and Accountability Act of 1996, referred to subsec. (d)(1)(C)(ii), is section 264(c) of Pub. L. 104-191, which is set out as a note under section 1320d-2 of Title 42, The Public Health and Welfare.

The Health Information Technology for Economic and Clinical Health Act, referred to in subsec. (d)(1)(C)(iii), is title XIII of div. A and title IV of div. B of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 226, 467, also known as the HITECH Act. For complete classification of this Act to the Code, see Short Title of 2009 Amendment note set out under section 201 of Title 42, The Public Health and Welfare, and Tables.

## **§ 1534. Cybercrime**

Subject to the availability of appropriations, and in accordance with the comparable level of the General Schedule, the Attorney General and the Secretary of Homeland Security shall provide incentive pay, in an amount that is not more than 25 percent of the basic pay of the individual, to an individual appointed to a position in the Department of Justice (including the Federal Bureau of Investigation) or the Department of Homeland Security (including positions in Homeland Security Investigations), respectively, requiring significant cyber skills, including to aid in—

(1) the protection of trafficking victims;

(2) the prevention of trafficking in persons; or

(3) the prosecution of technology-facilitated crimes against children by buyers or traffickers in persons.

(Pub. L. 117-347, title IV, § 401, Jan. 5, 2023, 136 Stat. 6207.)

## **Editorial Notes**

### **REFERENCES IN TEXT**

The General Schedule, referred to in text, is set out under section 5332 of Title 5, Government Organization and Employees.

### **CODIFICATION**

Section was enacted as part of the Abolish Trafficking Reauthorization Act of 2022, and not as part of

the Cybersecurity Act of 2015 which comprises this chapter.