6 USCS § 663

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)

§ 663. Federal intrusion detection and prevention system

(a) Definitions. In this section—

(1) the term "agency" has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term "agency information" means information collected or maintained by or on behalf of an agency;

(3) the term "agency information system" has the meaning given the term in section 2210 [6 USCS § 660]; and

(4) [Deleted]

(b) Requirement.

(1) In general. Not later than 1 year after the date of enactment of this section [enacted Dec. 18, 2015], the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) Regular improvement. The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) Activities. In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or

prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) Principles. In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) Private entities.

(1) Conditions. A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) Limitation on liability. No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) Rule of construction. Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) Privacy Officer review. Not later than 1 year after the date of enactment of this section [enacted Dec. 18, 2015], the Privacy Officer appointed under section 222 [6 USCS § 142], in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

History

HISTORY:

Nov. 25, 2002, P. L. 107-296, Title XXII [II], Subtitle A [C], § 2213 [230], as added Dec. 18, 2015, P. L. 114-113, Div N, Title II, Subtitle B, § 223(a)(6), 129 Stat. 2964; Nov. 16, 2018, P.L. 115-278, § 2(g)(2)(I), (9)(A)(vii), 132 Stat. 4178, 4181; Dec. 23, 2022, P.L. 117-263, Div G, Title LXXI, Subtitle E, § 7143(b)(2)(H), 136 Stat. 3660.