(2) Coordination with the Inspector General

(A) In general

Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.

(B) Coordination

(i) Referral

Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.

(ii) Determinations and notifications by the Inspector General

(I) In general

Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(bb) notify the senior official of that determination.

(II) Investigation not initiated

If the Inspector General notifies the senior official under subclause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this subclause shall be made not later than 3 days after the end of that 90-day period.

(iii) Investigation by senior official

The senior official may investigate a matter referred under clause (i) if—

(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.

(iv) Privacy training

Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

(d) Notification to Congress on removal

If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and

(2) include in any such notification the reasons for the removal or transfer.

(e) Reports by senior official to Congress

The senior official appointed under subsection (a) shall—

(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

(Pub. L. 107–296, title II, §222, Nov. 25, 2002, 116 Stat. 2155; Pub. L. 108–458, title VIII, §8305, Dec. 17, 2004, 118 Stat. 3868; Pub. L. 110–53, title VIII, §802, Aug. 3, 2007, 121 Stat. 358.)

Editorial Notes

REFERENCES IN TEXT

The Privacy Act of 1974, referred to in subsec. (a)(2), (6), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.

AMENDMENTS

2007—Pub. L. 110–53 designated existing provisions as subsec. (a), inserted heading, and added subsecs. (b) to (e).

2004—Pub. L. 108–458, §8305(1), inserted ‘‘, who shall report directly to the Secretary,’’ after ‘‘in the Department’’ in introductory provisions.

Pars. (5), (6). Pub. L. 108–458, §8305(2)–(4), added par. (5) and redesignated former par. (5) as (6).

§§ 143 to 145. Transferred

Editorial Notes

CODIFICATION

Section 143, Pub. L. 107–296, title II, §223, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(A), Aug. 3, 2007, 121 Stat. 334; Pub. L. 113–283, §2(e)(3)(A), Dec. 18, 2014, 128 Stat. 3086, which related to enhancement of Federal and non-Federal cybersecurity, was renumbered section 2205 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 655 of this title.

Section 144, Pub. L. 107–296, title II, §224, Nov. 25, 2002, 116 Stat. 2156; Pub. L. 110–53, title V, §531(b)(1)(B), Aug.

3, 2007, 121 Stat. 334, which related to NET Guard, was renumbered section 2206 of Pub. L. 107–296 by Pub. L. 115–278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 656 of this title.

Section 145, Pub. L. 107–296, title II, § 225, Nov. 25, 2002, 116 Stat. 2156, which related to Cyber Security Enhancement Act of 2002, was renumbered section 2207 of Pub. L. 107–296 by Pub. L. 115–278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 657 of this title.

§ 146. Cybersecurity workforce assessment and strategy

(a) Workforce assessment

(1) In general

Not later than 180 days after December 18, 2014, and annually thereafter for 3 years, the Secretary shall assess the cybersecurity workforce of the Department.

(2) Contents

The assessment required under paragraph (1) shall include, at a minimum—

(A) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;

(B) information on where cybersecurity workforce positions are located within the Department;

(C) information on which cybersecurity workforce positions are—

(i) performed by—

(I) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about such employees;

(II) independent contractors; and

(III) individuals employed by other Federal agencies, including the National Security Agency; or

(ii) vacant; and

(D) information on—

(i) the percentage of individuals within each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and

(ii) in cases in which such essential training was not received, what challenges, if any, were encountered with respect to the provision of such essential training.

(b) Workforce strategy

(1) In general

The Secretary shall—

(A) not later than 1 year after December 18, 2014, develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and

(B) maintain and, as necessary, update the comprehensive workforce strategy developed under subparagraph (A).

(2) Contents

The comprehensive workforce strategy developed under paragraph (1) shall include a description of—

(A) a multi-phased recruitment plan, including with respect to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

(B) a 5-year implementation plan;

(C) a 10-year projection of the cybersecurity workforce needs of the Department;

(D) any obstacle impeding the hiring and development of a cybersecurity workforce in the Department; and

(E) any gap in the existing cybersecurity workforce of the Department and a plan to fill any such gap.

(c) Updates

The Secretary submit[1] to the appropriate congressional committees annual updates on—

(1) the cybersecurity workforce assessment required under subsection (a); and

(2) the progress of the Secretary in carrying out the comprehensive workforce strategy required to be developed under subsection (b).

(Pub. L. 113–246, § 3, Dec. 18, 2014, 128 Stat. 2880.)

Editorial Notes

CODIFICATION

Section was enacted as part of the Cybersecurity Workforce Assessment Act, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

Statutory Notes and Related Subsidiaries

HOMELAND SECURITY CYBERSECURITY WORKFORCE ASSESSMENT

Pub. L. 113–277, § 4, Dec. 18, 2014, 128 Stat. 3008, provided that:

''(a) SHORT TITLE.—This section may be cited as the 'Homeland Security Cybersecurity Workforce Assessment Act'.

''(b) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Committee on Homeland Security of the House of Representatives; and

''(C) the Committee on House Administration of the House of Representatives.

''(2) CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPECIALTY AREA.—The terms 'Cybersecurity Work Category', 'Data Element Code', and 'Specialty Area' have the meanings given such terms in the Office of Personnel Management's Guide to Data Standards.

''(3) DEPARTMENT.—The term 'Department' means the Department of Homeland Security.

''(4) DIRECTOR.—The term 'Director' means the Director of the Office of Personnel Management.

''(5) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

''(c) NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.—

''(1) IN GENERAL.—The Secretary shall—

''(A) identify all cybersecurity workforce positions within the Department;

''(B) determine the primary Cybersecurity Work Category and Specialty Area of such positions; and

''(C) assign the corresponding Data Element Code, as set forth in the Office of Personnel Management's Guide to Data Standards which is aligned with the National Initiative for Cybersecurity Edu-

[1] So in original.