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.

cation's National Cybersecurity Workforce Framework report, in accordance with paragraph (2).

''(2) EMPLOYMENT CODES.—

''(A) PROCEDURES.—Not later than 90 days after the date of the enactment of this Act [Dec. 18, 2014], the Secretary shall establish procedures—

''(i) to identify open positions that include cybersecurity functions (as defined in the OPM Guide to Data Standards); and

''(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

''(B) CODE ASSIGNMENTS.—Not later than 9 months after the date of the enactment of this Act, the Secretary shall assign the appropriate employment code to—

''(i) each employee within the Department who carries out cybersecurity functions; and

''(ii) each open position within the Department that have been identified as having cybersecurity functions.

''(3) PROGRESS REPORT.—Not later than 1 year after the date of the enactment of this Act, the Director shall submit a progress report on the implementation of this subsection to the appropriate congressional committees.

''(d) IDENTIFICATION OF CYBERSECURITY SPECIALTY AREAS OF CRITICAL NEED.—

''(1) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to subsection (c)(2)(B), and annually through 2021, the Secretary, in consultation with the Director, shall—

''(A) identify Cybersecurity Work Categories and Specialty Areas of critical need in the Department's cybersecurity workforce; and

''(B) submit a report to the Director that—

''(i) describes the Cybersecurity Work Categories and Specialty Areas identified under subparagraph (A); and

''(ii) substantiates the critical need designations.

''(2) GUIDANCE.—The Director shall provide the Secretary with timely guidance for identifying Cybersecurity Work Categories and Specialty Areas of critical need, including—

''(A) current Cybersecurity Work Categories and Specialty Areas with acute skill shortages; and

''(B) Cybersecurity Work Categories and Specialty Areas with emerging skill shortages.

''(3) CYBERSECURITY CRITICAL NEEDS REPORT.—Not later than 18 months after the date of the enactment of this Act, the Secretary, in consultation with the Director, shall—

''(A) identify Specialty Areas of critical need for cybersecurity workforce across the Department; and

''(B) submit a progress report on the implementation of this subsection to the appropriate congressional committees.

''(e) GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.—The Comptroller General of the United States shall—

''(1) analyze and monitor the implementation of subsections (c) and (d); and

''(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.''

DEFINITIONS

Pub. L. 113–246, §2, Dec. 18, 2014, 128 Stat. 2880, provided that: ''In this Act [enacting this section and provisions set out as a note under section 101 of this title]—

''(1) the term 'Cybersecurity Category' means a position's or incumbent's primary work function involving cybersecurity, which is further defined by Specialty Area;

''(2) the term 'Department' means the Department of Homeland Security;

''(3) the term 'Secretary' means the Secretary of Homeland Security; and

''(4) the term 'Specialty Area' means any of the common types of cybersecurity work as recognized by the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report.''

§§ 147 to 151. Transferred

Editorial Notes

CODIFICATION

Section 147, Pub. L. 107–296, title II, §226, as added Pub. L. 113–277, §3(a), Dec. 18, 2014, 128 Stat. 3005, which related to cybersecurity recruitment and retention, was renumbered section 2208 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 658 of this title.

Section 148, Pub. L. 107–296, title II, §227, formerly §226, as added Pub. L. 113–282, §3(a), Dec. 18, 2014, 128 Stat. 3066; renumbered §227 and amended Pub. L. 114–113, div. N, title II, §§203, 223(a)(3), Dec. 18, 2015, 129 Stat. 2957, 2963; Pub. L. 114–328, div. A, title XVIII, §1841(b), Dec. 23, 2016, 130 Stat. 2663, which related to national cybersecurity and communications integration center, was renumbered section 2209 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 659 of this title.

A prior section 227 of Pub. L. 107–296, as added by Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070, was classified to section 149 of this title prior to redesignation by Pub. L. 114–113 as section 228(c) of Pub. L. 107–296, and was classified to section 149(c) of this title prior to further redesignation by Pub. L. 115–278 as section 2210(c) of Pub. L. 107–296, which is classified to section 660(c) of this title.

Section 149, Pub. L. 107–296, title II, §228, as added and amended Pub. L. 114–113, div. N, title II, §§205, 223(a)(2), (4), (5), Dec. 18, 2015, 129 Stat. 2961, 2963, 2964, which related to cybersecurity plans, was renumbered section 2210 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 660 of this title.

A prior section 228 of Pub. L. 107–296 was renumbered section 229 and was classified to section 150 of this title prior to renumbering as section 2212, which is classified to section 662 of this title.

Section 149a, Pub. L. 107–296, title II, §228A, as added Pub. L. 114–328, div. A, title XIX, §1912(a), Dec. 23, 2016, 130 Stat. 2683, which related to cybersecurity strategy, was renumbered section 2211 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 661 of this title.

Section 150, Pub. L. 107–296, title II, §229, formerly §228, as added Pub. L. 113–282, §7(a), Dec. 18, 2014, 128 Stat. 3070; renumbered §229, Pub. L. 114–113, div. N, title II, §223(a)(1), Dec. 18, 2015, 129 Stat. 2963, which related to clearances, was renumbered section 2212 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 662 of this title.

Section 151, Pub. L. 107–296, title II, §230, as added Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964, which related to Federal intrusion detection and prevention system, was renumbered section 2213 of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178, and transferred to section 663 of this title.

PART C—OFFICE OF SCIENCE AND TECHNOLOGY

Editorial Notes

CODIFICATION

Subtitle D of title II of Pub. L. 107–296, which was classified to part D of this subchapter, was redesignated subtitle C of title II of Pub. L. 107–296 by Pub. L. 115–278, §2(g)(2)(K), Nov. 16, 2018, 132 Stat. 4178, and transferred to this part.