IN THE SENATE OF THE UNITED STATES

JULY 29, 2014

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

To require the Secretary of Homeland Security to establish cybersecurity occupation classifications, assess the cybersecurity workforce, develop a strategy to address identified gaps in the cybersecurity workforce, and for other purposes.

Be it enacted by the Senate and House of Representa-

tives of the United States of America in Congress assembled,
SECTION 1. HOMELAND SECURITY CYBERSECURITY WORKFORCE.

(a) In General.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

“SEC. 226. CYBERSECURITY OCCUPATION CATEGORIES, WORKFORCE ASSESSMENT, AND STRATEGY.

“(a) Short Title.—This section may be cited as the ‘Homeland Security Cybersecurity Boots-on-the-Ground Act’.

“(b) Cybersecurity Occupation Categories.—

“(1) In General.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop and issue comprehensive occupation categories for individuals performing activities in furtherance of the cybersecurity mission of the Department.

“(2) Applicability.—The Secretary shall ensure that the comprehensive occupation categories issued under paragraph (1) are used throughout the Department and are made available to other Federal agencies.

“(c) Cybersecurity Workforce Assessment.—

“(1) In General.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary shall assess the
readiness and capacity of the workforce of the Department to meet its cybersecurity mission.

“(2) CONTENTS.—The assessment required under paragraph (1) shall, at a minimum, include the following:

“(A) Information where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories issued under subsection (b).

“(B) Information on which cybersecurity positions are—

“(i) performed by—

“(I) permanent full time departmental employees, together with demographic information about such employees’ race, ethnicity, gender, disability status, and veterans status;

“(II) individuals employed by independent contractors; and

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

“(ii) vacant.

“(C) The number of individuals hired by the Department pursuant to the authority
granted to the Secretary in 2009 to permit the
Secretary to fill 1,000 cybersecurity positions
across the Department over a three year period,
and information on what challenges, if any,
were encountered with respect to the implement-
tation of such authority.

“(D) Information on vacancies within the
Department’s cybersecurity supervisory work-
force, from first line supervisory positions
through senior departmental cybersecurity posi-
tions.

“(E) Information on the percentage of in-
dividuals within each cybersecurity occupation
category who received essential training to per-
form their jobs, and in cases in which such
training is not received, information on what
challenges, if any, were encountered with re-
spect to the provision of such training.

“(F) Information on recruiting costs in-
curred with respect to efforts to fill cybersecu-
rity positions across the Department in a man-
ner that allows for tracking of overall recruiting
and identifying areas for better coordination
and leveraging of resources within the Depart-
ment.
“(d) **Workforce Strategy.**—

“(1) **In general.**—Not later than 180 days after the date of the enactment of this section, the Secretary shall develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department.

“(2) **Contents.**—The comprehensive workforce strategy developed under paragraph (1) shall include—

“(A) a multiphased recruitment plan, including relating 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 Department’s cybersecurity workforce needs; and

“(D) obstacles impeding the hiring and development of a cybersecurity workforce at the Department.

“(e) **Information Security Training.**—Not later than 270 days after the date of the enactment of this section, the Secretary shall establish and maintain a process to verify on an ongoing basis that individuals employed
by independent contractors who serve in cybersecurity po-
sitions at the Department receive initial and recurrent in-
formation security training comprised of general security
awareness training necessary to perform their job func-
tions, and role-based security training that is commensu-
rate with assigned responsibilities. The Secretary shall
maintain documentation to ensure that training provided
to an individual under this subsection meets or exceeds
requirements for such individual’s job function.

“(f) UPDATES.—The Secretary shall submit to the
appropriate congressional committees annual updates re-
garding the cybersecurity workforce assessment required
under subsection (c), information on the progress of car-
rying out the comprehensive workforce strategy developed
under subsection (d), and information on the status of the
implementation of the information security training re-
quired under subsection (e).

“(g) GAO STUDY.—The Secretary shall provide the
Comptroller General of the United States with information
on the cybersecurity workforce assessment required under
subsection (c) and progress on carrying out the com-
prehensive workforce strategy developed under subsection
(d). The Comptroller General shall submit to the Sec-
retary and the appropriate congressional committees a
study on such assessment and strategy.
“(h) CYBERSECURITY FELLOWSHIP PROGRAM.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 225 the following new item:

“Sec. 226. Cybersecurity occupation categories, workforce assessment, and strategy.”.

SEC. 2. PERSONNEL AUTHORITIES.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by section 1 of this Act, is further amended by adding at the end the following new section:

“SEC. 227. PERSONNEL AUTHORITIES.

“(a) IN GENERAL.—

“(1) PERSONNEL AUTHORITIES.—The Secretary may exercise with respect to qualified employees of the Department the same authority that the Secretary of Defense has with respect to civilian intelligence personnel and the scholarship program under sections 1601, 1602, 1603, and 2200a of title
10, United States Code, to establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed under this section if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus under this paragraph, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a written explanation of such determination. Such authority shall be exercised—

“(A) to the same extent and subject to the same conditions and limitations that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense; and

“(B) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

“(2) **Civil Service Protections.**—Sections 1221 and 2302, and chapter 75 of title 5, United States Code, shall apply to the positions established pursuant to the authorities provided under paragraph (1).
“(3) Plan for execution of authorities.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a plan for the use of the authorities provided under this subsection.

“(b) Annual report.—Not later than one year after the date of the enactment of this section and annually thereafter for four years, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a detailed report (including appropriate metrics on actions occurring during the reporting period) that discusses the processes used by the Secretary in implementing this section and accepting applications, assessing candidates, ensuring adherence to veterans’ preference, and selecting applicants for vacancies to be filled by a qualified employee.

“(c) Definition of qualified employee.—In this section, the term ‘qualified employee’ means an employee who performs functions relating to the security of Federal civilian information systems, critical infrastruc-
ture information systems, or networks of either of such systems.”.

(b) Clerical Amendment.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 226 (as added by section 1 of this Act) the following new item:

“Sec. 227. Personnel authorities.”.

SEC. 3. CLARIFICATION REGARDING AUTHORIZATION OF APPROPRIATIONS.

No additional amounts are authorized to be appropriated by reason of this Act or the amendments made by this Act.

Passed the House of Representatives July 28, 2014.

Attest: KAREN L. HAAS,

Clerk.