

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 3107
OFFERED BY MS. CLARKE OF NEW YORK**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Homeland Security
3 Cybersecurity Boots-on-the-Ground Act”.

**4 SEC. 2. CYBERSECURITY OCCUPATION CLASSIFICATIONS,
5 WORKFORCE ASSESSMENT, AND STRATEGY.**

6 (a) CYBERSECURITY OCCUPATION CLASSIFICA-
7 TIONS.—

8 (1) IN GENERAL.—Not later than 90 days after
9 the date of the enactment of this Act, the Secretary
10 of Homeland Security shall develop and issue com-
11 prehensive occupation classifications for individuals
12 performing activities in furtherance of the cybersecu-
13 rity mission of the Department of Homeland Secu-
14 rity.

15 (2) APPLICABILITY.—The Secretary of Home-
16 land Security shall ensure that the comprehensive
17 occupation classifications issued under subsection (a)
18 may be used throughout the Department of Home-

1 land Security and are made available to other Fed-
2 eral agencies.

3 (b) CYBERSECURITY WORKFORCE ASSESSMENT.—

4 (1) IN GENERAL.—Not later than 180 days
5 after the date of the enactment of this Act, the Sec-
6 retary of Homeland Security, acting through the
7 Chief Human Capital Officer and Chief Information
8 Officer of the Department of Homeland Security,
9 shall assess the readiness and capacity of the De-
10 partment to meet its cybersecurity mission.

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

14 (A) Information where cybersecurity posi-
15 tions are located within the Department of
16 Homeland Security, specified in accordance
17 with the cybersecurity occupation classifications
18 issued under subsection (a).

19 (B) Information on which cybersecurity po-
20 sitions are—

21 (i) performed by—

22 (I) permanent full time depart-
23 mental employees, together with de-
24 mographic information about such

1 employees' race, ethnicity, gender, dis-
2 ability status, and veterans status;

3 (II) individuals employed by inde-
4 pendent contractors; and

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

8 (ii) vacant.

9 (C) The number of individuals hired by the
10 Department pursuant to the authority granted
11 to the Secretary of Homeland Security in 2009
12 to permit the Secretary to fill 1,000 cybersecu-
13 rity positions across the Department over a
14 three year period, and information on what
15 challenges, if any, were encountered with re-
16 spect to the implementation of such authority.

17 (D) Information on vacancies within the
18 Department's cybersecurity supervisory work-
19 force, from first line supervisory positions
20 through senior departmental cybersecurity posi-
21 tions.

22 (E) Information on the percentage of indi-
23 viduals within each cybersecurity occupation
24 classification who received essential training to
25 perform their jobs, and in cases in which such

1 training is not received, information on what
2 challenges, if any, were encountered with re-
3 spect to the provision of such training.

4 (F) Information on recruiting costs in-
5 curred with respect to efforts to fill cybersecu-
6 rity positions across the Department in a man-
7 ner that allows for tracking of overall recruiting
8 and identifying areas for better coordination
9 and leveraging of resources within the Depart-
10 ment.

11 (c) WORKFORCE STRATEGY.—

12 (1) IN GENERAL.—Not later than 180 days
13 after the date of the enactment of this Act, the Sec-
14 retary of Homeland Security shall develop a com-
15 prehensive workforce strategy that enhances the
16 readiness, capacity, training, and recruitment and
17 retention of the cybersecurity workforce of the De-
18 partment of Homeland Security.

19 (2) CONTENTS.—The comprehensive workforce
20 strategy developed under paragraph (1) shall in-
21 clude—

22 (A) a multiphased recruitment plan;

23 (B) a 5-year implementation plan; and

24 (C) a 10-year projection of Federal work-
25 force needs.

1 (d) INFORMATION SECURITY TRAINING.—Not later
2 than 270 days after the date of the enactment of this Act,
3 the Secretary of Homeland Security shall establish and
4 maintain a process to verify on an ongoing basis that indi-
5 viduals employed by independent contractors who serve in
6 cybersecurity positions at the Department of Homeland
7 Security receive initial and recurrent information security
8 training comprised of general security awareness training
9 necessary to perform their job functions, and role-based
10 security training that is commensurate with assigned re-
11 sponsibilities. The Secretary shall maintain documentation
12 to ensure that training provided to an individual under
13 this subsection meets or exceeds requirements for such in-
14 dividual’s job function.

15 (e) UPDATES.—Together with the submission to Con-
16 gress of annual budget requests, the Secretary of Home-
17 land Security shall provide updates regarding the cyberse-
18 curity workforce assessment required under subsection
19 (b), information on the progress of carrying out the com-
20 prehensive workforce strategy developed under subsection
21 (c), and information on the status of the implementation
22 of the information security training required under sub-
23 section (d).

24 (f) GAO STUDY.—The Secretary of Homeland Secu-
25 rity shall provide the Comptroller General of the United

1 States with information on the cybersecurity workforce as-
2 sessment required under subsection (a) and progress on
3 carrying out the comprehensive workforce strategy devel-
4 oped under subsection (c). The Comptroller General shall
5 submit to the Secretary, the Committee on Homeland Se-
6 curity of the House of Representatives, and the Committee
7 on Homeland Security and Governmental Affairs of the
8 Senate a study on such assessment and strategy.

9 **SEC. 3. DEFINITION.**

10 In this Act, the term “cybersecurity mission” means
11 activities that encompass the full range of threat reduc-
12 tion, vulnerability reduction, deterrence, incident response,
13 resiliency, and recovery activities to foster the security and
14 stability of cyberspace.

