AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

113TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
113–294

HOMELAND SECURITY CYBERSECURITY BOOTS-ON-THE-GROUND ACT

DECEMBER 12, 2013.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 3107]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3107) 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, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Homeland Security Cybersecurity Boots-on-the-Ground Act".

SEC. 2. CYBERSECURITY OCCUPATION CLASSIFICATIONS, WORKFORCE ASSESSMENT, AND STRATEGY.

(a) CYBERSECURITY OCCUPATION CLASSIFICATIONS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop and issue comprehensive occupation classifications for individuals performing activities in furtherance of the cybersecurity mission of the Department of Homeland Security.

(2) APPLICABILITY.—The Secretary of Homeland Security shall ensure that the comprehensive occupation classifications issued under paragraph (1) are used throughout the Department of Homeland Security and are made available to other Federal agencies.

(b) CYBERSECURITY WORKFORCE ASSESSMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Chief Human Capital Officer and Chief Information Officer of the Department of Homeland Security, shall assess the readiness and capacity 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 of Homeland Security, specified in accordance with the cybersecurity occupation classifications issued under subsection (a).

(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 of Homeland Security 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 implementation of such authority.

(D) Information on vacancies within the Department's cybersecurity supervisory workforce, from first line supervisory positions through senior departmental cybersecurity positions.

(E) Information on the percentage of individuals within each cybersecurity occupation classification who received essential training to perform their jobs, and in cases in which such training is not received, information on what challenges, if any, were encountered with respect to the provision of such training.

(F) Information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department in a manner that allows for tracking of overall recruiting and identifying areas for better coordination and leveraging of resources within the Department.

(c) WORKFORCE STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of the cybersecurity workforce of the Department of Homeland Security.

(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; and

(C) a 10-year projection of Federal workforce needs.

(d) INFORMATION SECURITY TRAINING.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Homeland Security shall establish and maintain a process to verify on an ongoing basis that individuals employed by independent contractors who serve in cybersecurity positions at the Department of Homeland Security receive initial and recurrent information security training comprised of general security awareness training necessary to perform their job functions, and role-based security training that is commensurate 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.

(e) UPDATES.—Together with the submission to Congress of annual budget requests, the Secretary of Homeland Security shall provide updates regarding the cybersecurity workforce assessment required under subsection (b), information on the progress of carrying out the comprehensive workforce strategy developed under subsection (c), and information on the status of the implementation of the information security training required under subsection (d).

(f) GAO STUDY.—The Secretary of Homeland Security shall provide the Comptroller General of the United States with information on the cybersecurity workforce assessment required under subsection (a) and progress on carrying out the comprehensive workforce strategy developed under subsection (c). The Comptroller General shall submit to the Secretary, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a study on such assessment and strategy.

SEC. 3. CYBERSECURITY FELLOWSHIP PROGRAM.

Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security 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 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 of Homeland Security for an agreed-upon period of time.

SEC. 4. DEFINITION.

In this Act, the term "cybersecurity mission" means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, incident response, resiliency, and recovery activities to foster the security and stability of cyberspace.

CONTENTS

PURPOSE AND SUMMARY

The purpose of H.R. 3107 is 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.

BACKGROUND AND NEED FOR LEGISLATION

The Department of Homeland Security (DHS) is responsible for the prevention of, and defense against threats to United States cybersecurity. Such threats come in many forms and include threats to individuals, corporations, and the Government. The events of September 11, 2001, demonstrate that terrorist attacks on the homeland can occur in unconventional ways and result in unanticipated consequences to national security posture and economic vitality. The U.S. is fortunate enough to have an extensive cybersecurity workforce, and this workforce is the first line of defense that keeps Americans safe, secure, and free from many cyber attacks. However, gaps in this workforce still expose vulnerabilities in our Nation's ability to reduce cyber threats, deter and respond to incidents, and recover from cyberattacks. The Committee notes that the Government Accountability Office reported that more than one in five jobs at a key cybersecurity component within the Department are vacant.

The Committee also notes that the cadre of professionals with cyber mission-critical skills is limited and Federal agencies have to compete among themselves and private sector employers for staff-

ing. Recognizing this challenge, the Homeland Security Advisory Committee (HSAC) 'Task Force on CyberSkills' issued a series of recommendations that include the adoption and maintenance an authoritative list of mission-critical cybersecurity tasks and the adoption of a sustainable model for assessing the competency and progress of the existing and future DHS mission-critical cybersecurity workforce.

It is therefore necessary that DHS develop a comprehensive workforce assessment and strategy to address gaps in the Nation's cybersecurity workforce.

The Committee believes that this strategy will enhance the readiness, capacity, training, and recruitment and retention of DHS's cybersecurity workforce. Legislation is required for DHS to develop such a workforce assessment and strategy, identify gaps in the cybersecurity workforce, provide information security training, and establish and encourage necessary coordination and collaboration across the Department. H.R. 3107, the Homeland Security Cybersecurity Boots-on-the-Ground Act, is bipartisan legislation developed from valuable input from stakeholders across government and industry.

This bill provides four major provisions that will help identify gaps in the cybersecurity workforce. First, the bill directs DHS to develop and issue comprehensive occupation classifications for persons performing activities in furtherance of the Department's cybersecurity missions. Second, the bill requires the Secretary, acting through the Chief Human Capital Officer and Chief Information Officer of the Department, to assess the readiness and capacity of the Department to meet its cybersecurity mission. As a part of the assessment, the Department has to identify where positions are located, whether these positions are vacant, held by full-time employees, or contractors. Additionally, it requires the Department to report on the extent to which it has exercised special hiring authority to fill cyber positions. Third, the bill requires the Secretary to develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of the Department's cybersecurity workforce. Finally, the bill requires the Secretary to establish and maintain a process to verify that individuals employed by independent contractors who serve in cybsersecurity positions at the Department receive initial and recurrent information security training.

HEARINGS

No hearings were held on H.R. 3107. However, the Committee held oversight hearings on programs and threats that are directly relevant to H.R. 3107. Those hearings are listed below.

112th Congress.

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing on April 15, 2011, entitled "The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure." The Subcommittee received testimony from Mr. Sean McGurk, Director, National Cybersecurity and Communications Integration Center, Department of Homeland Security; Mr. Gerry Cauley, President and CEO, North American Electric Reliability Corporation; Ms. Jane Carlin, Chair, Financial

Services Sector Coordinating Council; and Mr. Edward Amoroso, Senior Vice President and Chief Security Officer, AT&T.

On April 24, 2012, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "America is Under Cyber Attack: Why Urgent Action is Needed." The Subcommittee received testimony from Mr. Shawn Henry, Former Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, Federal Bureau of Investigation, Department of Justice; Mr. James Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies; Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; Mr. Stuart McClure, Chief Technology Officer, McAfee; and Dr. Stephen E. Flynn, Founding Co-Director, George J. Kostas Research Institute for Homeland Security, Northeastern University.

113th Congress.

On March 13, 2013, the Committee held a hearing entitled "DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure." The Committee received testimony from Hon. Jane Holl Lute, Deputy Secretary, U.S. Department of Homeland Security; Mr. Anish B. Bhimani, Chairman, Financial Services Information Sharing and Analysis Center; Mr. Gary W. Hayes, Chief Information Officer, Centerpoint Energy; and Ms. Michelle Richardson, Legislative Counsel, American Civil Liberties Union.

On May 16, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities." The Subcommittee received testimony from Ms. Roberta Stempfley, Acting Assistant Secretary, Office of Cybersecurity and Communications, U.S. Department of Homeland Security; Mr. Larry Zelvin, Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security; and Mr. Charles K. Edwards, Acting Inspector General, U.S. Department of Homeland Security.

On October 30, 2013, the Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a joint hearing entitled "Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management." The Subcommittee received testimony from Ms. Roberta Stempfley, Acting Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; Mr. Charley English, Director, Georgia Emergency Management Agency, *testifying on behalf of the National Emergency Management Association*; Mr. Craig Orgeron, Chief Information Officer and Executive Director, Department of Information Technology Services, State of Mississippi, *testifying on behalf of the National Association of State Chief Information Officers*; Mr. Mike Sena, Deputy Director, Northern California Regional Intelligence Center, *testifying on behalf of the National Fusion Center Association*; and Mr. Paul Molitor, Assistant Vice President, National Electrical Manufacturers Association.

COMMITTEE CONSIDERATION

The Committee on Homeland Security met on October 29, 2013, to consider H.R. 3107, and ordered the measure to be reported to the House with a favorable recommendation by voice vote. The Committee took the following actions:

The Committee agreed to H.R. 3107, as amended, by voice vote. The following amendments were offered:

An Amendment in the Nature of a Substitute to H.R. 3107 offered by MS. CLARKE (#1); was AGREED TO, as amended, by voice vote.

A unanimous consent request by Mr. McCaul to consider the Amendment in the Nature of a Substitute as base text for purposes of amendment was not objected to.

An amendment to the Amendment in the Nature of a Substitute to H.R. 3107 offered by MS. JACKSON LEE (#1A); was WITHDRAWN by unanimous consent.

Add at the end of paragraph (2) of section 2(b) the following: (G) Information on how many senior, mid- and entry level cybersecurity positions are filled by career Federal employees and how many are filled by contractors.; was WITHDRAWN by unanimous consent.

An amendment to the Amendment in the Nature of a Substitute to H.R. 3107 offered by MS. JACKSON LEE (#1B); was AGREED TO by voice vote.

Add at the end of section 2 a new subsection entitled "(g) Cybersecurity Fellowship Program."

An amendment to the Amendment in the Nature of a Substitute to H.R. 3107 offered by MR. KEATING (#1C); was AGREED TO by voice vote.

In paragraph (2) of section 2(a), strike "may be" and insert "are".

An amendment to the Amendment in the Nature of a Substitute to H.R. 3107 offered by MR. SWALWELL (#1D); was AGREED TO by voice vote.

In subparagraph (A) of section 2(c)(1), insert before the semicolon at the end the following: ", including relating to mid-career employees, members of economically disadvantaged or underserved communities, the unemployed, and veterans".

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies met on September 18, 2013, to consider H.R. 3107, and reported the measure to the Full Committee with a favorable recommendation, amended, by voice vote. The Subcommittee took the following actions:

The following amendments were offered:

An en bloc amendment offered by MR. MEEHAN (#1); was AGREED TO by voice vote.

Consisting of the following amendments:

In subparagraph (A) of section 2(c), strike "and" at the end.

In section 2(c), redesignate subparagraph (B) as subparagraph (C).

In section 2(c), insert after subparagraph (A) the following:

(B) a five-year implementation plans; and

In section 2, add at the end a new subsection entitled "(f) GAO Study."

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3107.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3107, the Homeland Security Cybersecurity Boots–on–the–Ground Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of Rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 3107 contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

The performance goals and objectives of H.R. 3107 are based on the development of a workforce assessment and strategy to improve and identify gaps in the DHS cybersecurity workforce. The goal of the workforce assessment required under H.R. 3107 is to help assess the readiness and capacity of the Department to meet its cybersecurity mission. The performance objective of the assessment is to provide information on vacancies within the Department's cybersecurity workforce, the percentage of cybersecurity individuals who received essential training to perform their jobs, and recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department. The goal of the workforce strategy required under H.R. 3107 is to enhance the readiness, capacity, training, and recruitment and retention of the cybersecurity workforce of the Department. The performance objective of this strategy is to develop a multi-phased recruitment plan, an implementation plan, and projection of Federal workforce needs as well as to provide information security training for independent contractors who serve in cybersecurity positions at the Department. The Congressional reports from DHS and GAO required by this Act will allow Congress to hold the Department accountable for the success or failure of its workforce assessment and strategy implementation.

DUPLICATIVE FEDERAL PROGRAMS

The Committee finds that H.R. 3107 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3107 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3107 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that the bill may be cited as the "Homeland Security Cybersecurity Boots-on-the-Ground-Act."

Sec. 2. Cybersecurity Occupation Classifications, Workforce Assessment, and Strategy.

(a) Cybersecurity Occupation Classifications.

This subsection requires the Secretary to develop and issue comprehensive occupation classifications for persons performing activities in furtherance of the Department's cybersecurity missions. The Secretary shall ensure that the classifications are used throughout the Department and made available to other Federal agencies. These comprehensive classifications must be made no later than 90 days after the enactment of this Act.

Based on extensive oversight, the Committee has found that there currently is no comprehensive occupation classification for the Department's cybsersecurity workforce. The Committee believes that the Department needs to provide necessary occupation classifications to better assess and develop a workforce strategy. TheCommittee intends that workforce occupation classifications are at the discretion of the Secretary so long as these classifications are consistent throughout the Department and made available to other Federal agencies. The Committee strongly encourages DHS to develop workforce categorizations that are consistent with those used by the public sector and other Federal agencies. The Committee furthermore strongly encourages DHS to implement workforce categorizations that are aligned to market-based salaried positions in order to attract and retain quality cybersecurity professionals.

(b) Cybersecurity Workforce Assessment.

This subsection requires the Secretary, acting through the Chief Human Capital Officer and Chief Information Officer of the Department, to assess the readiness and capacity of the Department to meet its cybersecurity mission. This assessment must be conducted no later than 180 days after the enactment of this Act. The assessment shall, at a minimum, include the following: Information where cybersecurity positions are located within the Department; information on which cybersecurity positions are performed by permanent full time departmental employees, individuals employed by independent contractors, and individuals employed by other Federal agencies; 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 over a three year period; information on vacancies within the Department's cybersecurity supervisory workforce; information on the percentage of individuals within each cybersecurity occupation classification who received essential training to perform their jobs; and information on recruiting costs incurred with respect to efforts to fill ybersecurity positions across the Department.

The contents of the assessment prescribed are the minimum contents required. However, the Committee strongly encourages DHS to include other aspects necessary for effective assessment of the cybersecurity workforce. The Committee expects that each of the prescribed elements of the assessment be developed and published in sufficient detail in order to enable DHS to create and implement a workforce strategy described in subsection (c) and identify any gaps in the cybersecurity workforce.

(c) Workforce Strategy.

In this subsection, the contents of the workforce strategy are prescribed. This subsection requires the Secretary, not later than 180

days after the enactment of this Act, to develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of the Department's cybersecurity workforce. This workforce strategy shall include a multiphased recruitment plan, a 5–year implementation plan, and a 10–year projection of Federal workforce needs. By including a specific timeframe, the Committee encourages DHS to address near-term, midterm, and long-term aspects of the plan. The workforce strategy is to be developed in a manner that is not constrained by fiscal resources to address both short-term and long-term strategies. The Committee furthermore expects DHS to write the strategy in an organized hierarchal manner structured around specified objectives, goals, and measures. The Committee also recognizes that strategies can change due to unforeseen circumstances, and encourages DHS to actively update and republish the strategy regularly as needed.

(d) Information Security Training.

This subsection sets forth the requirements for information security training of the cybersecurity workforce. It requires the Secretary to establish and maintain a process to verify that individuals employed by independent contractors who serve in cybsersecurity positions at the Department receive initial and recurrent information security training. The Committee believes that it is essential for the cybersecurity workforce to be properly trained in all areas necessary to protect cybersecurity. Such training is to include both general security awareness role-based security training. The Committee also believes that it is necessary for DHS to train all independent contractors so that the entire cybersecurity workforce, not just DHS employees, is adequately prepared to respond to or prevent threats and attacks. This subsection also requires that training include recurrent information training. It is the Committee's belief that recurrent training is necessary to ensure that the cybersecurity workforce is prepared to handle the continually changing nature of cyber threats and attacks. Lastly, this subsection requires that the Secretary shall maintain documentation to ensure that training provided to an individual meets or exceeds requirements for such individual's job function.

(e) Updates.

This subsection requires the Secretary to provide updates regarding the cybsersecurity workforce assessment, information on the progress of carrying out the comprehensive workforce strategy, and information on the status of the implementation of information security training. The Committee believes that updates are important to ensure development of the Department's cybersecurity workforce and to continually satisfy the workforce mission. The bill does not specify when updates must be given, and allows DHS flexibility in providing such information. However, the Committee believes that these updates are necessary to determine the progress and status of the implementation of the workforce assessment and strategy, as well as information security training. The Committee strongly encourages the Secretary to provide regular updates on a consistent basis.

(f) GAO Study.

This subsection requires the Secretary to provide the Comptroller General of the United States information on the cybersecurity workforce assessment and progress on carrying out the comprehensive workforce strategy developed. This subsection also requires the GAO to submit to the relevant Congressional committees a study on such assessment and strategies. The Committee's intent of this subsection is to direct GAO to gather data and evaluate DHS's workforce assessment and strategies. The Committee believes that the Department does not adequately meet its cybersecurity workforce needs and this independent assessment will inform the relevant Congressional committees of the Department's progress on addressing this issue. The GAO report will provide important inputs for continuing Congressional oversight and provide additional transparency for the American public.

Sec. 3. Definition.

In this section, the term "cybersecurity mission" is defined as activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, incident response, resiliency, and recovery activities to foster the security and stability of cyberspace. The Committee believes that determining the cybersecurity mission of the Department is essential to protecting critical infrastructure and developing a workforce that is able to prevent and respond to cyber threats and attacks. The purpose of defining cybsersecurity mission in this bill is to codify into statute the full range of activities necessary for the Department to fulfill when developing and assessing its cybersecurity workforce.

Since this bill only addresses the workforce assessment and strategy of cybersecurity, it is the Committee's intent that the basic definition described in this section suffice for such purposes. However, the Committee recognizes that cybersecurity missions have a significantly broader role in cybersecurity protection and threat reduction and that the definition herein may not suffice for these broader purposes. Therefore, the Committee strongly encourages the Secretary to develop a set of effective and efficient Departmental processes for cybersecurity missions that define, designate, and support the broader cybersecurity and critical infrastructure protection mission.

Sec. 4. Cybersecurity Fellowship Program.

This section requires the Secretary to 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. The Committee believes that, if feasible, a Cybersecurity Fellowship Program would help fill gaps in the cybersecurity workforce and provide recent graduates with career opportunities.

○