Executive Order 13870—America's Cybersecurity Workforce

May 2, 2019

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to better ensure continued American economic prosperity and national security, it is hereby ordered as follows:

Section 1. Policy. (a) America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The National Cyber Strategy, the President's 2018 Management Agenda, and Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), each emphasize that a superior cybersecurity workforce will promote American prosperity and preserve peace. America's cybersecurity workforce is a diverse group of practitioners who govern, design, defend, analyze, administer, operate, and maintain the data, systems, and networks on which our economy and way of life depend. Whether they are employed in the public or private sectors, they are guardians of our national and economic security.

(b) The United States Government must enhance the workforce mobility of America's cybersecurity practitioners to improve America's national cybersecurity. During their careers, America's cybersecurity practitioners will serve in various roles for multiple and diverse entities. United States Government policy must facilitate the seamless movement of cybersecurity practitioners between the public and private sectors, maximizing the contributions made by their diverse skills, experiences, and talents to our Nation.

(c) The United States Government must support the development of cybersecurity skills and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. The United States Government must also recognize and reward the country's highest-performing cybersecurity practitioners and teams.

(d) The United States Government must create the organizational and technological tools required to maximize the cybersecurity talents and capabilities of American workers –- especially when those talents and capabilities can advance our national and economic security. The Nation is experiencing a shortage of cybersecurity talent and capability, and innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities. Training opportunities, such as work-based learning, apprenticeships, and blended learning approaches, must be enhanced for both new workforce entrants and those who are advanced in their careers.

(e) In accordance with Executive Order 13800, the President will continue to hold heads of executive departments and agencies (agencies) accountable for managing cybersecurity risk to their enterprises, which includes ensuring the effectiveness of their cybersecurity workforces.

Sec. 2. Strengthening the Federal Cybersecurity Workforce. (a) To grow the cybersecurity capability of the United States Government, increase integration of the Federal cybersecurity workforce, and strengthen the skills of Federal information technology and cybersecurity practitioners, the Secretary of Homeland Security, in consultation with the Director of the Office of Management and Budget (OMB) and the Director of the Office of Personnel Management (OPM), shall establish a cybersecurity rotational assignment program, which will

serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners. Within 90 days of the date of this order, the Secretary of Homeland Security, in consultation with the Directors of OMB and OPM, shall provide a report to the President that describes the proposed program, identifies its resource implications, and recommends actions required for its implementation. The report shall evaluate how to achieve the following objectives, to the extent permitted by applicable law, as part of the program:

(i) The non-reimbursable detail of information technology and cybersecurity employees, who are nominated by their employing agencies, to serve at the Department of Homeland Security (DHS);

(ii) The non-reimbursable detail of experienced cybersecurity DHS employees to other agencies to assist in improving those agencies' cybersecurity risk management;

(iii) The use of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) as the basis for cybersecurity skill requirements for program participants;

(iv) The provision of training curricula and expansion of learning experiences to develop participants' skill levels; and

(v) Peer mentoring to enhance workforce integration.

(b) Consistent with applicable law and to the maximum extent practicable, the Administrator of General Services, in consultation with the Director of OMB and the Secretary of Commerce, shall:

(i) Incorporate the NICE Framework lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services;

(ii) Ensure that contracts for information technology and cybersecurity services include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the NICE Framework; and

(iii) Provide a report to the President, within 1 year of the date of this order, that describes how the NICE Framework has been incorporated into contracts for information technology and cybersecurity services, evaluates the effectiveness of this approach in improving services provided to the United States Government, and makes recommendations to increase the effective use of the NICE Framework by United States Government contractors.

(c) Within 180 days of the date of this order, the Director of OPM, in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other agencies as appropriate, shall identify a list of cybersecurity aptitude assessments for agencies to use in identifying current employees with the potential to acquire cybersecurity skills for placement in reskilling programs to perform cybersecurity work. Agencies shall incorporate one or more of these assessments into their personnel development programs, as appropriate and consistent with applicable law.

(d) Agencies shall ensure that existing awards and decorations for the uniformed services and civilian personnel recognize performance and achievements in the areas of cybersecurity and cyber-operations, including by ensuring the availability of awards and decorations

equivalent to citations issued pursuant to Executive Order 10694 of January 10, 1957 (Authorizing the Secretaries of the Army, Navy, and Air Force To Issue Citations in the Name of the President of the United States to Military and Naval Units for Outstanding Performance in Action), as amended. Where necessary and appropriate, agencies shall establish new awards and decorations to recognize performance and achievements in the areas of cybersecurity and cyber-operations. The Assistant to the President for National Security Affairs may recommend to agencies that any cyber unified coordination group or similar ad hoc interagency group that has addressed a significant cybersecurity or cyber-operations-related national security crisis, incident, or effort be recognized for appropriate awards and decorations.

(e) The Secretary of Homeland Security, in consultation with the Secretary of Defense, the Director of the Office of Science and Technology Policy, the Director of OMB, and the heads of other appropriate agencies, shall develop a plan for an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines. The plan shall be submitted to the President within 90 days of the date of this order. The first competition shall be held no later than December 31, 2019, and annually thereafter. The plan for the competition shall address the following:

(i) The challenges and benefits of inviting advisers, participants, or observers from non-Federal entities to observe or take part in the competition and recommendations for including them in future competitions, as appropriate;

(ii) How the Department of Energy, through the National Laboratories, in consultation with the Administrator of the United States Digital Service, can provide expert technical advice and assistance to support the competition, as appropriate;

(iii) The parameters for the competition, including the development of multiple individual and team events that test cybersecurity skills related to the NICE Framework and other relevant skills, as appropriate. These parameters should include competition categories involving individual and team events, software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, cyber-physical systems, and other disciplines;

(iv) How to encourage agencies to select their best cybersecurity practitioners as individual and team participants. Such practitioners should include Federal employees and uniformed services personnel from Federal civilian agencies, as well as Department of Defense active duty military personnel, civilians, and those serving in a drilling reserve capacity in the Armed Forces Reserves or National Guard;

(v) The extent to which agencies, as well as uniformed services, may develop a President's Cup awards program that is consistent with applicable law and regulations governing awards and that allows for the provision of cash awards of not less than $25,000. Any such program shall require the agency to establish an awards program before allowing its employees to participate in the President's Cup Cybersecurity Competition. In addition, any such program may not preclude agencies from recognizing winning and non-winning participants through other means, including honorary awards, informal recognition awards, rating-based cash awards, time-off awards, Quality Step Increases, or other agency-based compensation flexibilities as appropriate and consistent with applicable law; and

(vi) How the uniformed services, as appropriate and consistent with applicable law, may designate service members who win these competitions as having skills at a time when there is a critical shortage of such skills within the uniformed services. The plan should also address how the uniformed services may provide winning service members with a combination of bonuses, advancements, and meritorious recognition to be determined by the Secretaries of the agencies concerned.

(f) The Director of OMB shall, in consultation with appropriate agencies, develop annually a list of agencies and subdivisions related to cybersecurity that have a primary function of intelligence, counterintelligence, investigative, or national security work, including descriptions of such functions. The Director of OMB shall provide this list to the President, through the Deputy Assistant to the President for Homeland Security and Counterterrorism (DAPHSCT), every year starting September 1, 2019, for consideration of whether those agencies or subdivisions should be exempted from coverage under the Federal Labor-Management Relations Program, consistent with the requirements of section 7103(b)(1) of title 5, United States Code.

Sec. 3. Strengthening the Nation's Cybersecurity Workforce. (a) The Secretary of Commerce and the Secretary of Homeland Security (Secretaries), in coordination with the Secretary of Education and the heads of other agencies as the Secretaries determine is appropriate, shall execute, consistent with applicable law and to the greatest extent practicable, the recommendations from the report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (Workforce Report) developed pursuant to Executive Order 13800. The Secretaries shall develop a consultative process that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners to assess and make recommendations to address national cybersecurity workforce needs and to ensure greater mobility in the American cybersecurity workforce. To fulfill the Workforce Report's vision of preparing, growing, and sustaining a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity, priority consideration will be given to the following imperatives:

(i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;

(ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;

(iii) To align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and

(iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

(b) To strengthen the ability of the Nation to identify and mitigate cybersecurity vulnerabilities in critical infrastructure and defense systems, particularly cyber-physical systems for which safety and reliability depend on secure control systems, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, and the Secretary of Homeland Security, in coordination with the Director of OPM and the Secretary of Labor, shall provide a report to the President, through the DAPHSCT, within 180 days of the date of this order that:

(i) Identifies and evaluates skills gaps in Federal and non-Federal cybersecurity personnel and training gaps for specific critical infrastructure sectors, defense critical

infrastructure, and the Department of Defense's platform information technologies; and

(ii) Recommends curricula for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

(c) Within 1 year of the date of this order, the Secretary of Education, in consultation with the DAPHSCT and the National Science Foundation, shall develop and implement, consistent with applicable law, an annual Presidential Cybersecurity Education Award to be presented to one elementary and one secondary school educator per year who best instill skills, knowledge, and passion with respect to cybersecurity and cybersecurity-related subjects. In developing and implementing this award, the Secretary of Education shall emphasize demonstrated superior educator accomplishment—without respect to research, scholarship, or technology development—as well as academic achievement by the educator's students.

(d) The Secretary of Commerce, the Secretary of Labor, the Secretary of Education, the Secretary of Homeland Security, and the heads of other appropriate agencies shall encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law. The Secretary of Commerce shall provide annual updates to the President regarding effective uses of the NICE Framework by non-Federal entities and make recommendations for improving the application of the NICE Framework in cybersecurity education, training, and workforce development.

Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

The White House,
May 2, 2019.

[Filed with the Office of the Federal Register, 11:15 a.m., May 8, 2019]

NOTE: This Executive order was published in the *Federal Register* on May 9.

Categories: Executive Orders : U.S. cybersecurity workforce, strengthening efforts.

Subjects: Defense and national security : Cybersecurity :: Strengthening efforts.

DCPD Number: DCPD201900266.