AMENDMENT TO RULES COMMITTEE PRINT

116–57

OFFERED BY MR. LANGEVIN OF RHODE ISLAND

At the end of title XI, add the following:

Subtitle C—Office of the National Cyber Director

SEC. 1131. SHORT TITLE.

This subtitle may be cited as the ''National Cyber Director Act''.

SEC. 1132. NATIONAL CYBER DIRECTOR.

(a) ESTABLISHMENT.—There is established, within the Executive Office of the President, the Office of the National Cyber Director (in this section referred to as the ''Office'').

(b) NATIONAL CYBER DIRECTOR.—

(1) IN GENERAL.—The Office shall be headed by the National Cyber Director (in this section referred to as the ''Director'') who shall be appointed by the President, by and with the advice and consent of the Senate. The Director shall hold office at the pleasure of the President, and shall be entitled to receive the same pay and allowances as are provided

for level I of the Executive Schedule under section 5312 of title 5, United States Code.

(2) DEPUTY DIRECTORS.—There shall be two Deputy National Cyber Directors, to be appointed by the President, who shall hold office at the pleasure of the President, and who shall report to the Director, as follows:

(A) The Deputy National Cyber Director for Strategy, Capabilities, and Budget.

(B) The Deputy National Cyber Director for Plans and Operations.

(c) DUTIES OF THE NATIONAL CYBER DIRECTOR.—

(1) IN GENERAL.—Subject to the authority, direction, and control of the President, the Director shall—

(A) serve as the principal advisor to the President on cybersecurity strategy and policy;

(B) in consultation with appropriate Federal departments and agencies, develop the United States' National Cyber Strategy, which shall include elements related to Federal departments and agencies—

(i) information security; and

(ii) programs and policies intended to improve the United States' cybersecurity posture;

(C) in consultation with appropriate Federal departments and agencies and upon approval of the National Cyber Strategy by the President, supervise implementation of the strategy by—

(i) in consultation with the Director of the Office of Management and Budget, monitoring and assessing the effectiveness, including cost-effectiveness, of Federal departments and agencies' implementation of the strategy;

(ii) making recommendations relevant to changes in the organization, personnel and resource allocation, and policies of Federal departments and agencies to the Director of the Office of Management and Budget and heads of such departments and agencies in order to implement the strategy;

(iii) reviewing the annual budget proposal for each Federal department or agency and certifying to the head of each Fed-

eral department or agency and the Director of the Office Management and Budget whether the department or agency proposal is consistent with the strategy;

(iv) continuously assessing and making relevant recommendations to the President on the appropriate level of integration and interoperability across the Federal cybersecurity operations centers;

(v) coordinating with the Federal Chief Information Officer, the Federal Chief Information Security Officer, the Director of the Cybersecurity and Infrastructure Security Agency, and the Director of National Institute of Standards and Technology on the development and implementation of policies and guidelines related to issues of Federal department and agency information security; and

(vi) reporting annually to the President and the Congress on the state of the United States' cybersecurity posture, the effectiveness of the strategy, and the status of Federal departments and agencies' implementation of the strategy;

(D) lead joint interagency planning for the Federal Government's integrated response to cyberattacks and cyber campaigns of significant consequence, to include—

(i) coordinating with relevant Federal departments and agencies in the development of, for the approval of the President, joint, integrated operational plans, processes, and playbooks for incident response that feature—

(I) clear lines of authority and lines of effort across the Federal Government;

(II) authorities that have been delegated to an appropriate level to facilitate effective operational responses across the Federal Government; and

(III) support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the United States' cybersecurity posture;

(ii) exercising these operational plans, processes, and playbooks;

(iii) updating these operational plans, processes, and playbooks for incident response as needed in coordination with ongoing offensive cyber plans and operations; and

(iv) ensuring these plans, processes, and playbooks are properly coordinated with relevant private sector entities, as appropriate;

(E) direct the Federal Government's response to cyberattacks and cyber campaigns of significant consequence, to include—

(i) developing for the approval of the President, with the heads of relevant Federal departments and agencies independently or through the National Security Council as directed by the President, operational priorities, requirements, and tasks;

(ii) coordinating, deconflicting, and ensuring the execution of operational activities in incident response; and

(iii) coordinating operational activities with relevant private sector entities;

(F) coordinate and consult with private sector leaders on cybersecurity and emerging technology issues with the support of, and in coordination with, the Cybersecurity and Infrastructure Security Agency and other Federal departments and agencies, as appropriate;

(G) annually report to Congress on cybersecurity threats and issues facing the nation, including any new or emerging technologies that may impact national security, economic prosperity, or enforcing the rule of law; and

(H) be responsible for such other functions as the President may direct.

(2) DELEGATION OF AUTHORITY.—The Director may—

(A) serve as the senior representative on any body that the President may establish for the purpose of providing the President advice on cybersecurity;

(B) be empowered to convene National Security Council, National Economic Council and Homeland Security Council meetings, with the concurrence of the National Security Advisor, Homeland Security Advisor, or Director of the National Economic Council, as appropriate;

(C) be included as a participant in preparations for and, if appropriate, execution of cybersecurity summits and other international meetings at which cybersecurity is a major topic;

(D) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as he may designate; and

(E) authorize such successive re-delegations of such functions, powers, and duties to such officers and employees of the Office as he may deem appropriate.

(d) ATTENDANCE AND PARTICIPATION IN NATIONAL SECURITY COUNCIL MEETINGS.—Section 101(c)(2) of the National Security Act of 1947 (50 U.S.C. 3021(c)(2)) is amended by striking ''and the Chairman of the Joint Chiefs of Staff'' and inserting ''the Chairman of the Joint Chiefs of Staff, and the National Cyber Director''.

(e) POWERS OF THE DIRECTOR.—The Director may, for the purposes of carrying out the Director's functions under this section—

(1) subject to the civil service and classification laws, select, appoint, employ, and fix the compensation of such officers and employees as are necessary

and prescribe their authority and duties, except that not more than 75 individuals may be employed without regard to any provision of law regulating the employment or compensation at rates not to exceed the basic rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5, United States Code;

(2) employ experts and consultants in accordance with section 3109 of title 5, United States Code, and compensate individuals so employed for each day (including travel time) at rates not in excess of the maximum rate of basic pay for grade GS-15 as provided in section 5332 of such title, and while such experts and consultants are so serving away from their homes or regular place of business, to pay such employees travel expenses and per diem in lieu of subsistence at rates authorized by section 5703 of such title 5 for persons in Federal Government service employed intermittently;

(3) promulgate such rules and regulations as may be necessary to carry out the functions, powers, and duties vested in the Director;

(4) utilize, with their consent, the services, personnel, and facilities of other Federal agencies;

(5) enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary in the conduct of the work of the Office and on such terms as the Director may determine appropriate, with any Federal agency, or with any public or private person or entity;

(6) accept voluntary and uncompensated services, notwithstanding the provisions of section 1342 of title 31, United States Code;

(7) adopt an official seal, which shall be judicially noticed; and

(8) provide, where authorized by law, copies of documents to persons at cost, except that any funds so received shall be credited to, and be available for use from, the account from which expenditures relating thereto were made.

(f) DEFINITIONS.—In this section:

(1) CYBERSECURITY POSTURE.—The term ''cybersecurity posture'' means the ability to identify and protect, and detect, respond to and recover from intrusions in, information systems the compromise of which could constitute a cyber attack or cyber campaign of significant consequence.

(2) CYBER ATTACKS AND CYBER CAMPAIGNS OF SIGNIFICANT CONSEQUENCE.—The term ''cyber at-

tacks and cyber campaigns of significant consequence'' means an incident or series of incidents that have the purpose or effect of—

(A) causing a significant disruption to the availability of a Federal information system;

(B) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(C) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(E) otherwise constituting a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

(3) INCIDENT.—The term ''incident'' has the meaning given that term in section 3552 of title 44, United States Code.

(4) INFORMATION SECURITY.—The term ''information security'' has the meaning given that term in section 3552 of title 44, United States Code.

☒