I

111TH CONGRESS
2D SESSION

H. R. 5247

To establish a National Cyberspace Office, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 6, 2010

Mr. LANGEVIN (for himself, Mr. MCCAUL, Mr. RODRIGUEZ, Mr. RUPPERSBERGER, Ms. CLARKE, Ms. LORETTA SANCHEZ of California, Ms. MARKEY of Colorado, and Mr. SMITH of Washington) introduced the following bill; which was referred to the Committee on Oversight and Government Reform, and in addition to the Committees on Armed Services and Select Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To establish a National Cyberspace Office, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Executive Cyberspace Authorities Act of 2010''.

SEC. 2. NATIONAL CYBERSPACE OFFICE.

(a) ESTABLISHMENT.—There is established within the Executive Office of the President an office to be known as the National Cyberspace Office.

(b) DIRECTOR.—There shall be at the head of the National Cyberspace Office a Director, who shall be appointed by the President by and with the advice and consent of the Senate. The Director of the National Cyberspace Office shall administer all functions under this section and collaborate to the extent practicable with the heads of appropriate agencies, the private sector, and international partners. The National Cyberspace Office shall serve as the principal office for coordinating issues relating to achieving an assured, reliable, secure, and survivable information infrastructure and related capabilities for the Federal Government.

(c) AUTHORITY AND FUNCTIONS OF THE DIRECTOR OF THE NATIONAL CYBERSPACE OFFICE.—

(1) DUTIES OF THE DIRECTOR.—The Director of the National Cyberspace Office shall—

(A) oversee agency information security policies and practices, including—

(i) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely

agency adoption of and compliance with such policies, principles, standards, and guidelines;

(ii) reviewing at least annually, and approving or disapproving, each agency budget relating to the protection of information technology submitted pursuant to subsection (d);

(iii) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(iv) coordinating information security policies and procedures with related information resources management policies and procedures;

(v) overseeing the operation of the Federal information security incident center required under section 3546 of title 44, United States Code; and

(vi) reporting to Congress not later than March 1 of each year on agency compliance with the requirements of this Act, including—

(I) a summary of the findings of the independent evaluation required by section 3545 of title 44, United States Code;

(II) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

(III) significant deficiencies in agency information security practices;

(IV) planned remedial action to address such deficiencies; and

(V) a summary of, and the views of the Director on, the report prepared by the National Institute of

Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

(B) encourage public-private working groups with representatives from relevant agencies and industry partners to increase information sharing and policy coordination efforts in order to reduce vulnerabilities in the national information infrastructure;

(C) coordinate the defense of information infrastructure operated by agencies in the case of a large-scale attack on information technology, as determined by the Director;

(D) establish a national strategy, in consultation with the Department of State, the United States Trade Representative, and the National Institute of Standards and Technology, to engage with the international community to set the policies, principles, standards, or guidelines for information security; and

(E) coordinate information security training for Federal employees with the Office of Personnel Management.

(2) CONSULTATION.—The head of each agency shall consult with the Director regarding information security policies and practices.

(3) EXPERTS AND CONSULTANTS.—The Director may procure temporary and intermittent services under section 3109(b) of title 5, United States Code.

(4) MEMBERSHIP ON THE NATIONAL SECURITY COUNCIL.—Section 101(a) of the National Security Act of 1947 (50 U.S.C. 402(a)) is amended—

(A) by redesignating paragraphs (7) and (8) as paragraphs (8) and (9), respectively; and

(B) by inserting after paragraph (6) the following:

''(7) the Director of the National Cyberspace Office;''.

(d) BUDGET APPROVAL.—

(1) SUBMISSION OF BUDGET.—The head of each agency shall submit to the Director of the National Cyberspace Office a budget each year for the following fiscal year relating to the protection of information technology for such agency, by a date determined by the Director that is before the submission of such budget by the head of the agency to the Office of Management and Budget.

(2) BUDGET APPROVAL.—The Director shall review and approve or disapprove the budget before the submission of such budget by the head of the agency to the Office of Management and Budget.

(3) BUDGET DISAPPROVAL.—If the Director disapproves a budget under paragraph (2), the Director shall transmit recommendations to the head of the agency for such budget.

(4) BUDGET SUBMISSION REQUIREMENTS.—Each budget submitted by the head of an agency pursuant to paragraph (1) shall include—

(A) a review of any threats to information technology for such agency;

(B) a plan to secure the information infrastructure for such agency based on threats to information technology, using the National Institute of Standards and Technology guidelines and recommendations;

(C) a review of compliance by such agency with any previous year plan described in subparagraph (B); and

(D) a report on the development of the credentialing process to enable secure authentication of identity and authorization for access

to the information infrastructure of such agency.

(5) CYBER SECURITY PERFORMANCE.—The National Cyberspace Office may recommend to the President that awards and bonuses be withheld for any agency that failed to make adequate efforts to secure the information infrastructure of such agency.

(e) NATIONAL SECURITY SYSTEMS.—Except for the authority described in clauses (iii) and (vi) of subsection (c)(1)(A), the authorities of the Director of the National Cyberspace Office under this section shall not apply to national security systems.

(f) DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS.—

(1) DELEGATION OF AUTHORITY.—The authority of the Director of the National Cyberspace Office described in subparagraphs (A)(i) and (C) of subsection (c)(1) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

(2) DEPARTMENT OF DEFENSE.—The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor

of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) CENTRAL INTELLIGENCE AGENCY.—The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

(g) CONFORMING AMENDMENTS.—Title 44, United States Code, is amended—

(1) in section 3546(a), by striking ''Director'' and inserting ''Director of the National Cyberspace Office''; and

(2) in section 3545(e)—

(A) in paragraph (1), by inserting ''and the Director of the National Cyberspace Office'' after ''submit to the Director''; and

(B) in paragraph (2), by inserting ''and the Director of the National Cyberspace Office'' after ''the Director''.

SEC. 3. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 3502 of title 44, United States Code.

(2) INFORMATION INFRASTRUCTURE.—The term ''information infrastructure'' means the underlying framework that information systems and assets rely on in processing, storing, or transmitting information electronically.

(3) INFORMATION RESOURCES MANAGEMENT.—The term ''information resources management'' has the meaning given that term in section 3502 of title 44, United States Code.

(4) INFORMATION SECURITY.—The term ''information security'' has the meaning given that term in section 3542 of title 44, United States Code.

(5) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given that term in section 11101 of title 40, United States Code.

(6) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given that term in section 3542 of title 44, United States Code.

○