114TH CONGRESS
1ST SESSION

S. 1828

To strengthen the ability of the Secretary of Homeland Security to detect and prevent intrusions against, and to use countermeasures to protect, Government agency information systems, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 22, 2015

Ms. COLLINS (for herself, Mr. WARNER, Ms. MIKULSKI, Mr. COATS, Ms. AYOTTE, and Mrs. MCCASKILL) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To strengthen the ability of the Secretary of Homeland Security to detect and prevent intrusions against, and to use countermeasures to protect, Government agency information systems, 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 ''Federal Information Security Management Reform Act of 2015''.

SEC. 2. DUTIES OF THE SECRETARY OF HOMELAND SECURITY RELATED TO INFORMATION SECURITY.

Section 3553(b)(6) of title 44, United States Code, is amended by striking subparagraphs (B), (C), and (D) and inserting the following:

''(B) operating consolidated intrusion detection, prevention, or other protective capabilities and use of associated countermeasures for the purpose of protecting agency information and information systems from information security threats;

''(C) providing incident detection, analysis, mitigation, and response information and remote or onsite technical assistance to the head of an agency;

''(D) compiling and analyzing data on agency information security;

''(E) developing and conducting targeted risk assessments and operational evaluations for agency information and information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments;

''(F) in conjunction with other agencies and the private sector, assessing and fostering

the development of information security technologies and capabilities for use across multiple agencies; and

"(G) coordinating with appropriate agencies and officials to ensure, to the maximum extent feasible, that policies and directives issued under paragraph (2) are complementary with—

"(i) standards and guidelines developed for national security systems; and

"(ii) policies and directives issued by the Secretary of Defense and the Director of National Intelligence under subsection (e)(1); and".

SEC. 3. COMMUNICATIONS AND SYSTEM TRAFFIC AND DIRECTION TO AGENCIES.

Section 3553 of title 44, United States Code, is amended by adding at the end the following:

"(h) COMMUNICATIONS AND SYSTEMS TRAFFIC.—

"(1) IN GENERAL.—

"(A) ACQUISITION BY THE SECRETARY.—Notwithstanding any other provision of law and subject to subparagraph (B), in carrying out the responsibilities under subparagraphs (B), (C), and (E) of subsection (b)(6), if the Secretary makes a certification described in para-

graph (2), the Secretary may acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on agency information systems and deploy countermeasures with regard to the communications and system traffic.

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a communication or other system traffic that is transiting to or from or stored on a system described in paragraph (2) or (3) of subsection (e).

''(C) DISCLOSURE BY FEDERAL AGENCY HEADS.—The head of a Federal agency or department is authorized to disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (A), information traveling to or from or stored on an agency information system, notwithstanding any other law that would otherwise restrict or prevent agency heads from disclosing such information to the Secretary.

''(2) CERTIFICATION.—A certification described in this paragraph is a certification by the Secretary that—

''(A) the acquisitions, interceptions, and other countermeasures are reasonably necessary for the purpose of protecting agency information systems from information security threats;

''(B) the content of communications will be retained only if the communication is associated with a known or reasonably suspected information security threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with the threats;

''(C) information obtained under activities authorized under this subsection will only be retained, used, or disclosed to protect agency information systems from information security threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed;

''(D) notice has been provided to users of agency information systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic; and

''(E) the activities are implemented pursuant to policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications and other system traffic that have been reviewed and approved by the Attorney General.

''(3) PRIVATE ENTITIES.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities that provide electronic communication or information security services to acquire, intercept, retain, use, and disclose communications and other system traffic in accordance with this subsection.

''(4) NO CAUSE OF ACTION.—No cause of action shall exist against a private entity for assistance provided to the Secretary in accordance with paragraph (3).

''(i) DIRECTION TO AGENCIES.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—Notwithstanding section 3554, and subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary

may issue a directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems owned or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described in paragraph (2) or (3) of subsection (e).

''(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

''(A) in coordination with the Director and in consultation with Federal contractors, as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

''(i) thresholds and other criteria;

''(ii) privacy and civil liberties protections; and

''(iii) providing notice to potentially affected third parties;

''(B) specify the reasons for the required action and the duration of the directive;

''(C) minimize the impact of a directive under this subsection by—

''(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

''(ii) limiting directives to the shortest period practicable; and

''(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection.

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—If the Secretary determines that there is an imminent threat to agency information systems and a directive under this subsection is not reasonably likely to result in a timely response to the threat, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system

without prior consultation with the affected agency for the purpose of ensuring the security of the information or information system or other agency information systems.

''(B) LIMITATION ON DELEGATION.—The authority under this paragraph may not be delegated to an official in a position lower than an Assistant Secretary of the Department of Homeland Security.

''(C) NOTICE.—The Secretary shall immediately notify the Director and the head and chief information officer (or equivalent official) of each affected agency of—

''(i) any action taken under this subsection; and

''(ii) the reasons for and duration and nature of the action.

''(D) OTHER LAW.—Any action of the Secretary under this paragraph shall be consistent with applicable law.

''(4) LIMITATION.—The Secretary may direct or authorize lawful action or protective capability under this subsection only to—

''(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

''(B) require the remediation of or protect against identified information security risks with respect to—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.''.

SEC. 4. REPORT TO CONGRESS REGARDING OFFICE OF MANAGEMENT AND BUDGET ENFORCEMENT ACTION.

Section 3553 of title 44, United States Code, as amended by section 3, is further amended by inserting at the end the following new subsection:

''(j) ANNUAL REPORT TO CONGRESS.—

''(1) REQUIREMENT.—Not later than February 1 of every year, the Director shall report to the appropriate congressional committee regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to paragraph (5) of title 40 of section 11303(b).

''(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—In this subsection, the term 'appropriate congressional committee' means—

''(A) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(B) the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.''.

○